ASISA GUIDELINES ON THE PROTECTION OF PERSONAL INFORMATION

First published: July 2021

Last updated: March 2024

Page

PART 1 - INTERPRETATION AND INTRODUCTION

1 DEFINITIONS AND INTERPRETATION 3
2 INTRODUCTION 5
3 NATURE OF THE GUIDELINES 6
4 SCOPE 6

PART 2 - INFORMATION OFFICERS

5 INFORMATION OFFICERS 7

PART 3 - CONDITIONS FOR PROCESSING PERSONAL INFORMATION

6 ACCOUNTIBILITY 8
7 LAWFULNESS OF PROCESSING 8
8 MINIMALITY 9
9 CONSENT, JUSTIFICATION AND OBJECTION 10
10 COLLECTION DIRECTLY FROM DATA SUBJECTS 19
11 COLLECTION FOR A SPECIFIC PURPOSE 23
12 RECORD RETENTION 24
13 COMPATIBLE PURPOSE 31
14 INFORMATION QUALITY 34
15 DOCUMENTS 34
16 NOTIFICATIONS TO THE DATA SUBJECTS 34

PART 4 - SECURITY SAFEGUARDS

17 SECURITY MEASURES ON INTEGRITY OF PERSONAL INFORMATION 38
18 RESPONSIBLE PARTIES AND OPERATORS 40
19 NOTIFICATION OF SECURITY COMPROMISES 47

PART 5 - DATA SUBJECTS' PARTICIPATION

20 ACCESS TO PERSONAL INFORMATION 49
21 CORRECTION AND DESTRUCTION OF PERSONAL INFORMATION 50

PART 6 - PROCESSING OF SPECIAL PERSONAL INFORMATION

22 PROHIBITION ON PROCESSING OF SPECIAL PERSONAL INFORMATION 52
23 GENERAL EXEMPTIONS 53
24 SPECIAL EXEMPTIONS 54

PART 7 - PERSONAL INFORMATION OF CHILDREN

25 PROCESSING OF PERSONAL INFORMATION OF CHILDREN **57**

PART 8 - PRIOR AUTHORISATION

26 PROCESSING SUBJECT TO PRIOR AUTHORISATION **58**

PART 9 - UNSOLICITED ELECTRONIC COMMUNICATION, COOKIES AND AUTOMATED DECISION MAKING

27 ELECTRONIC DIRECT MARKETING **60**

28 COOKIES **63**

29 DECISIONS BASED ON THE AUTOMATED PROCESSING OF PERSONAL INFORMATION **64**

PART 10 - CROSS BORDER TRANSFERS

30 TRANSFERS OF PERSONAL INFORMATION OUTSIDE SOUTH AFRICA **65**

PART 11 - COMPLAINTS AND OFFENCES

31 COMPLAINTS **67**

32 UNLAWFUL ACTS BY RESPONSIBLE PARTIES IN CONNECTION WITH ACCOUNT NUMBERS **67**

PART 1 – INTERPRETATION AND INTRODUCTION

1. DEFINITIONS AND INTERPRETATION

1.1. In these Guidelines, unless otherwise defined herein, the following terms have the meanings assigned to them below:

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

1.1.2. "**Child**" has the meaning ascribed thereto in POPIA, namely a natural person under the age of 18 years who is not legally competent, without the assistance of a Competent Person, to take any action or decision in respect of any matter concerning him- or herself and "**Children**" has a similar meaning;

1.1.3. "**Competent Person**" has the meaning ascribed thereto in POPIA, namely any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a Child;

1.1.4. "**Consent**" has the meaning ascribed thereto in POPIA, namely any voluntary, specific and informed expression of will in terms of which permission is given for the Processing of Personal Information, and "**Consenting**" has a similar meaning;

1.1.5. "**Data Subject**" has the meaning ascribed thereto in POPIA, namely the person to whom Personal Information relates;

1.1.6. "**Direct Marketing**" has the meaning ascribed thereto in POPIA, namely to approach a Data Subject, either in person or by mail or Electronic Communication, for the direct or indirect purpose of:

1.1.6.1. promoting or offering to supply, in the ordinary course of business, any goods or services to the Data Subject; or

1.1.6.2. requesting the Data Subject to make a donation of any kind for any reason;

1.1.7. "**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;

1.1.8. "**Electronic Direct Marketing**" means Direct Marketing by means of unsolicited Electronic Communication;

1.1.9. "**FICA**" means the Financial Intelligence Centre Act, No. 38 of 2001;

1.1.10. "**Guidelines**" means the guidance on the protection of Personal Information as contained in this document;

1.1.11. "**Information Officer**" has the meaning ascribed thereto in POPIA in relation to a private body, namely the head of a private body as contemplated in section 1 of PAIA;

1.1.12. "**Operator**" has the meaning ascribed thereto in POPIA, namely 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;

1.1.13. "**PAIA**" means the Promotion of Access to Information Act, No. 2 of 2000;

1.1.14. "**Personal Information**" has the meaning ascribed thereto in POPIA, namely information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

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

1.1.14.2. information relating to the education or the medical, financial, criminal or employment history of the person;

1.1.14.3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

1.1.14.4. the biometric information of the person;

1.1.14.5. the personal opinions, views or preferences of the person;

1.1.14.6. 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;

1.1.14.7. the views or opinions of another individual about the person; and

1.1.14.8. 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;

1.1.15. "**POPIA**" means the Protection of Personal Information Act, No. 4 of 2013;

1.1.16. "**Privacy Notice**" means the disclosures to be provided to a Data Subject in accordance with section 18 of POPIA;

1.1.17. "**Process**" or "**Processing**" has the meaning ascribed thereto in POPIA[1], namely any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

1.1.17.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

1.1.17.2. dissemination by means of transmission, distribution or making available in any other form; or

1.1.17.3. merging, linking, as well as restriction, degradation, erasure or destruction of information;

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

1.1.19. "**Responsible Party**" has the meaning ascribed thereto in POPIA, namely 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

1.1.20. "**Special Personal Information**" has the meaning ascribed thereto in POPIA, namely 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.

1.2. Any reference to "*you*" or "*your*" in these Guidelines refers to your organisation acting as a Responsible Party.

1.3. Where these Guidelines use the word "*must*", this means that the law requires you to do something (so it's a legal requirement). Where the word "*should*" or "*recommend*" is used this is considered important to help you comply and it is recommended that you follow this unless you have a good reason not to (good practice). However, you may take a different approach and still comply. Where the words "can", "*could*" or "*may*" are used, this refers to an option(s) that you may want to consider to help you comply.

2. INTRODUCTION

2.1. All ASISA members are committed to the protection of Personal Information. These Guidelines have accordingly been established in the interests of promoting the protection of Personal Information in the savings and investment industry.

[1] The definition of "*processing*" in POPIA is very wide and covers almost anything a Responsible Party will do with Personal Information.

2.2. The Guidelines, which are published on the ASISA website, also serve to enhance transparency about how POPIA may be practically applied in the savings and investment industry.

3. NATURE OF THE GUIDELINES

3.1. All ASISA members that are in scope in terms of paragraph 4 may participate in these Guidelines.

3.2. These Guidelines are being shared with ASISA members and the public at large for their consideration and voluntary implementation.

3.3. Whilst the Guidelines may serve as useful background to the industry as to how Personal Information should be protected, they are non-binding and each ASISA member ought to take their own independent views and decisions as to how they wish to protect Personal Information and implement POPIA requirements.

4. SCOPE

4.1. The Guidelines are intended for use by the following Responsible Parties:

4.1.1. persons who carry on "life insurance business" as defined in the Insurance Act, No. 18 of 2017;

4.1.2. persons who are authorised in terms of the Collective Investment Schemes Control Act, No. 45 of 2002 ("**CISCA**") to administer collective investment schemes, excluding property unit trusts; and

4.1.3. category II (excluding brokers registered with the Johannesburg Stock Exchange), IIA and III financial service providers as defined in the Financial Advisory and Intermediary Services Act, No. 37 of 2002 ("**FAIS**").

4.2. Although registered pension fund administrators under section 13B of the Pension Funds Act, No. 24 of 1956 ("**PFA**") are acting primarily as Operators of Responsible Parties for purposes of POPIA, where a person who is conducting such business also falls under the scope of the Responsible Parties listed in paragraph 4.1, they may also follow the Guidelines in conducting their business as pension fund administrators.

4.3. The Guidelines are intended to apply to the Processing of Personal Information of Data Subjects by Responsible Parties insofar as the Processing is conducted within the ambit of their business activities as providers of financial products and/or services. These Guidelines do not lend themselves out to the following Processing of Personal Information:

4.3.1. the Processing of Personal Information by Responsible Parties in their capacity as employers;

4.3.2. the Processing of Personal Information relating to suppliers, vendors, contractors or service providers of Responsible Parties; and

4.3.3. the Processing of Personal Information by Responsible Parties in their capacity as Operators for other Responsible Parties.

Guidance note

- Each company within a group is a separate legal entity and, as such, qualifies as a separate Responsible Party.

PART 2 – INFORMATION OFFICERS

5. INFORMATION OFFICERS

5.1. Your Information Officer is by default the head of your organisation (being the CEO or equivalent officer) or any person duly authorised[2] by the head to be the organisation's information officer as contemplated in section 1 of PAIA. Each Responsible Party must register its own Information Officer with the Regulator.

5.2. Each Information Officer must designate[3] as many deputy information officers as may be required to ensure the Information Officer is able to fulfil his/her duties, and deputy information officers must be registered as such with the Regulator.

5.3. The Information Officer is responsible for performing the duties set out in POPIA[4] and Regulation 4. The Information Officer has the powers vested in him/her by POPIA and PAIA.[5]

Guidance notes

- In the context of group companies, the heads of different Responsible Parties in the group may authorise and register the same individual as its Information Officer to the effect that there is a single Information Officer for the various Responsible Parties in the group. That Information Officer may delegate his/her responsibilities to deputy Information Officers in the various Responsible Parties to enable the Information Officer to be sufficiently informed about the Processing of Personal

[2] Such authorisation must be affected by way of a written authorisation, substantially similar to the form attached as Annexure B to the Regulator's Guidance Note on Information Officers and Deputy Information Officers.
[3] Designation must be in the form of Annexure C to the Regulator's Guidance Note on Information Officers and Deputy Information Officers.
[4] Section 55(1).
[5] Section 55.

Information conducted in the respective Responsible Parties and to effectively fulfil his/her obligations under POPIA.

- Regard should be had to the Regulator's Guidance Note on Information Officers and Deputy Information Officers.

PART 3 – CONDITIONS FOR PROCESSING PERSONAL INFORMATION

6. ACCOUNTABILITY

6.1. The accountability condition requires you to take responsibility for what you do with Personal Information and how you comply with the other conditions for Processing.

Guidance notes

- Taking accountability means that every person in your organisation, from the top down, commits to their specific tasks and acknowledges their specific role in achieving compliance with POPIA.
- You should have appropriate measures and evidence in place to be able to demonstrate your compliance.
- It is helpful to establish an accountability framework which identifies the areas your organisation is accountable for and includes a checklist against which to measure your compliance. Topics such as the following may be included in such a framework: leadership and oversight; policies and procedures; training and awareness; individual's rights; transparency; records of Processing and lawful basis; contracts and data sharing; risks and data protection impact assessments; records management and security; and breach response and monitoring.

PROCESSING LIMITATION

7. LAWFULNESS OF PROCESSING

7.1. Personal Information must be Processed lawfully and in a reasonable manner that does not infringe the privacy of Data Subjects.[6]

Guidance note

- When Processing Personal Information, you should not only comply with POPIA, but should also take other applicable laws into consideration, for example other legislation and regulation and the common law. If any other legislation provides

[6] Section 9.

for the protection of Personal Information that is more extensive than provided for in POPIA, the more extensive provisions prevail.

8. MINIMALITY

8.1. You must ensure that the Personal Information that you Process is, given the purpose for which it is Processed:

8.1.1. adequate – sufficient to properly fulfil the state purpose;

8.1.2. relevant – has a rational link to that purpose; and

8.1.3. not excessive – i.e. not more than is needed for that purpose.[7]

Guidance notes

- The accountability condition means that you would need to be able to demonstrate that you have appropriate processes to ensure that you only collect and hold the Personal Information you need.
- It is recommended that you:
  - identify the minimum amount of Personal Information you need to fulfil your purpose and hold that much information, but no more;
  - not hold Personal Information on the off chance that it may be useful in the future;
  - periodically review your Processing to check that the Personal Information you hold is still relevant and adequate for its purposes and delete anything you no longer need.
- Personal Information should also be sufficient for the purpose for which it is collected - too little Personal Information may make it difficult to properly fulfil your purpose.
- The words "*adequate, relevant and not excessive*" *should* 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 you are holding the right amount of Personal Information, you should accordingly first establish why you are holding and using it.

Example

- You need to locate a beneficiary. You collect information on several people with a similar name to the beneficiary. During the enquiry some of these people are discounted. You should delete most of their Personal Information, keeping only the minimum data needed to form a basic record of a person you have removed from

[7] Section 10.

your search. It is appropriate to keep this small amount of information so that these people are not contacted again about benefits which do not belong to them.

9. CONSENT, JUSTIFICATION AND OBJECTION

Grounds for Processing

9.1. You must have a valid lawful basis in order to Process Personal Information.

9.2. There are six available lawful bases for Processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the Data Subject.

Consent

General

9.3. You 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.

9.4. "*Consent*" is defined in POPIA as "*any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information*".[8][9]

9.5. Consent should be capable of being withdrawn freely and without detriment to Data Subjects, provided that the lawfulness of the Processing of Personal Information before such withdrawal or the Processing of Personal Information on other lawful grounds will not be affected. Data Subjects must be informed of this right and the consequences of withdrawing Consent.

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.
- You should ensure that Consent you obtain:
  - is **voluntary** – the Data Subject should genuinely have a free choice, for example consent for Direct Marketing should not be a pre-condition for a product or service;
  - is **informed** – your purposes should be specific and 'granular' so that you get separate Consent for separate things. Vague or blanket consent is not enough;

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

- **expresses the Data Subject's will** – this refers to the act of giving permission. The Data Subject's consent must be expressed in some form or another, although the specific format in which such expression is communicated may differ as required by the relevant circumstances. How this consent will be expressed, will have to be determined in each case. This could include ticking a tick box, choosing technical settings, clicking on a link or being given an easy way to opt out.
- Consent should be specific to each purpose. An unspecific (general) authorisation to Process Personal Information which is not aimed at specific information and specific purposes of Processing will not be valid. Even if a new purpose is considered 'compatible' with an original purpose, this does not override the need for Consent to be specific.

- Consent requests are prominent, unbundled from other terms and conditions clearly distinguished by a heading, concise, easy to understand and user-friendly;
- It is recommended that you refresh:
  - existing consents that don't meet the POPIA requirements;
  - Consents where you have relied on Consent by a Competent Person, as children grow up and can give their own Consent;
  - Consents if your Processing operations or purposes evolve and your consents may no longer be fit for purpose.
- Any third-party Responsible Parties who will be relying on the Consent should be named – defined categories of third parties may not be acceptable under the POPIA definition.
- Consent does not have to be in writing, but written Consent has evidentiary value. If verbal Consent is obtained, it is recommended as a good practice to record the Consent.
- If for any reason you cannot offer people a genuine choice over how you use their information, Consent will not be the appropriate basis for Processing. This may be the case if, for example, you would still Process the information on a different lawful basis if Consent were refused or withdrawn, as seeking Consent from the Data Subject is misleading and inherently unfair. It presents the Data Subject with a false choice and only the illusion of control. You should identify the most appropriate lawful basis from the start.
- If Consent is withdrawn, Processing for the purpose for which Consent was obtained should stop. The relevant Personal Information may be processed for a different purpose where a different lawful basis was relied upon (and the Data Subject should have been informed of that at the time Consent was obtained). You cannot, however, change the lawful basis of the Processing for that purpose (for example to legitimate interests). When consent is used as a lawful basis for Processing, this gives the Data Subject a sense of control over the use of their Personal Information. To continue to Process the Personal Information for the same purpose after Consent is withdrawn would make that sense illusory and this would be unfair.

Examples

- A company that provides credit cards asks its customers to give Consent for their Personal Information to be sent to credit reference agencies for credit scoring. However, if a customer refuses or withdraws their Consent, the credit card company will still send the information to the credit reference agencies on the basis of 'legitimate interests'. So asking for Consent is misleading and inappropriate – there is no real choice. The company should have relied on 'legitimate interests' from the start. To ensure fairness and transparency, the company must still tell customers this will happen, but this is very different from giving them a choice in information protection terms.
- A company decides that it wants to use its customer database to market individuals. The customers have not previously Consented to receiving marketing messages so the company sends a letter to customers stating that it intends to send them details of special offers by post and email. The letter provides a number for customers to call if they don't want to receive marketing. Non-response would not constitute valid consent for marketing. Failure to call the number to opt-out will not satisfy the requirement that Data Subjects provide an indication signifying agreement. The company will not therefore be able to market its customers on this basis.

Consent for Electronic Direct Marketing

9.6. Please refer to section 8, paragraph 27 of the Guidelines.

Consent for Processing Special Personal Information

9.7. Please refer to section 6 of the Guidelines.

Necessary for performance of a contract

9.8. You may Process Personal Information if it is necessary to conclude or perform in terms of a contract to which the Data Subject is a party.[10]

Guidance notes

- You can rely on this lawful basis if:
  - you have a contract with the Data Subject and you need to Process their Personal Information to comply with your obligations under the contract;
  - you have a contract with the Data Subject and you need to Process their Personal Information so that they can comply with specific counter-obligations under the contract (e.g. you are Processing payment details);
  - you haven't yet got a contract with the Data Subject, but they have asked

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

you to do something as a first step (e.g. provide a quote) and you need to Process their Personal Information to do what they ask. This applies even if they don't actually go on to enter into a contract with you, as long as the Processing was in the context of a potential contract with that person.

- "*Necessary*" does not mean that the Processing must be absolutely essential or 'the only way' to perform the contract or take relevant pre-contractual steps. However, it should be more than just useful, and more than just part of your standard terms. It should be a targeted and proportionate step which is integral to delivering the contractual service or taking the requested action.
- Note that, in this context, a contract does not have to be a formal signed document, or even written down, as long as there is an agreement which meets the requirements of contract law. Broadly speaking, this means that the terms have been offered and accepted, you both intend them to be legally binding, and there is an element of exchange (usually an exchange of goods or services for money, but this can be anything of value).
- Even if you are not party to the contract, but it is necessary that you Processes Personal Information for the performance of a contract between the Data Subjects and another party such Processing is allowed.

Examples

- You Processes Personal Information contained in an application for an insurance or investment contract.
- You Process Personal Information about potential customers in order to conduct an affordability test.
- You are a retirement fund that has to pay out a beneficiary or next of kin on the death of the member. The beneficiary or next of kin isn't party to the agreement between yourself (as the fund) and the member, but you have to Process the beneficiary's Personal Information to give effect to the contract between yourself and the member.

Legal obligation

9.9. You may Process Personal Information if such Processing complies with an obligation imposed on you by law.[11]

9.10. You may rely on this lawful basis if you need to Process the Personal Information to comply with a common law or statutory obligation.

9.11. The Processing must be necessary. If you can reasonably comply without Processing the Personal Information, this basis does not apply.

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

Guidance notes

- This does not mean that there must be a legal obligation specifically requiring the specific Processing activity. The point is that your overall purpose should be to comply with a legal obligation.
- Before providing information to third parties, you should check whether the request for information is based on an obligation imposed by law.
- Although the Processing need not be essential for you to comply with the legal obligation, it should be a reasonable and proportionate way of achieving compliance. You should not rely on this lawful basis if you have discretion over whether to Process the Personal Information, or if there is another reasonable way to comply.
- This basis does not apply to contractual obligations.

Examples

- You Process Personal Information in order to comply with FICA or anti-money laundering obligations.
- You provide Personal Information to regulators or public bodies in terms of applicable legislation.
- You provide Personal information to the various Ombud schemes.
- Processing is conducted to comply with court orders or subpoenas.
- Personal information provided to SARS in terms of the Income Tax Act, No. 58 of 1962 ("**Income Tax Act**").
- You are required to trace "*dependants*" as defined in the PFA.

Legitimate interests of the Data Subject

9.12. You may Process Personal Information if the Processing protects a legitimate interest of the Data Subject.[12]

Guidance notes

- POPIA does not define "*legitimate interest*" and no guidance has been issued by the Regulator regarding its interpretation and no case law on this issue currently exists. Relying on its ordinary grammatical meaning, something that is legitimate is allowed under the law or reasonable and acceptable. This should include any interest that provides a clear benefit to the Data Subject. The Processing must be necessary. If you can reasonably protect the Data Subject's legitimate interests in another less intrusive way, this basis should not apply.
- You should consider whether you are likely to rely on this basis, and, if so, document the circumstances where it will be relevant and ensure you can justify your

[12] Section 11(1)(d).

reasoning.

- You should not rely on legitimate interest for health data or other Special Personal Information if the Data Subject is capable of giving Consent, even if they refuse their Consent.

Examples

- You Process the Personal Information of a person appointed as a beneficiary on a policy in order to pay the benefits to that person.
- You Process Personal Information to protect someone's life or other vital interests.

Public law duty

9.13. Personal information may be Processed if such Processing is necessary for the proper performance of a public law duty by a public body.[13]

Guidance note

- You cannot rely on another Responsible Party's public tasks, functions or powers as the lawful basis for your Processing, including disclosing Personal Information to them.

Example

- A government agency has statutory powers to conduct research about financial products. The agency asks financial institutions to share the Personal Information of a random sample of their customers to enable it to carry out this function. It explains that it will process the information under 'public task' once it receives the information. As the financial institutions are not subject to the agency's statutory function, they cannot share the information on the basis of the agency's public task. The financial institution may consider disclosing the information under another lawful basis, e.g. legitimate interests of a third party, but it should be borne in mind that the other conditions of lawful Processing must still be complied with, e.g. further Processing limitations.

Legitimate interests of the Responsible Party or a third party

9.14. You may Process Personal Information if this is necessary to pursue your or the legitimate interests of a third party to whom the information is supplied.[14]

9.15. There are two elements to the legitimate interest basis. It helps to think of this as a two-part test. You must:

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

9.15.1. identify that a legitimate interest is being pursued; and

9.15.2. show that the Processing is necessary to achieve it.

Guidance notes

- The term "*necessary*" means that the condition will not be met if you can reasonably achieve the same result in another less intrusive way.
- It is good practice to balance your legitimate interests against those of the Data Subject by conducting a legitimate interest assessment based on the specific context and circumstances:
  - Firstly, you should identify the legitimate interest(s). Consider:
    - Why do you want to Process the information – what are you trying to achieve?
    - Who benefits from the Processing? In what way?
    - Are there any wider public benefits to the Processing?
    - How important are those benefits?
    - What would the impact be if you couldn't go ahead?
    - Would your use of the information be unethical or unlawful in any way?
  - Secondly, you should apply the necessity test. Consider:
    - Does this Processing actually help to further that interest?
    - Is it a reasonable way to go about it?
    - Is there another less intrusive way to achieve the same result?
  - Thirdly, you should do a balancing test. Consider the impact of your Processing and whether this overrides the interest you have identified. You might find it helpful to think about the following:
    - What is the nature of your relationship with the Data Subject?
    - Is any of the information particularly sensitive or private?
    - Would people expect you to use their information in this way?
    - Are you happy to explain it to them?
    - Are some people likely to object or find it intrusive?
    - What is the possible impact on the Data Subject?
    - How big an impact might it have on them?
    - Are you Processing Children's information?
    - Are any of the Data Subject vulnerable in any other way?
    - Can you adopt any safeguards to minimise the impact?
    - Can you offer an opt-out?
  - You should then make a decision about whether you still think legitimate

interests is an appropriate basis. There's no foolproof formula for the outcome of the balancing test, but you should be confident that your legitimate interests are not overridden by the risks you have identified.

- It is recommended that you document assessments of your legitimate interest and keep a record of it to ensure you can justify your decision.
- The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.
- You should avoid using legitimate interests if you are using Personal Information in ways Data Subject do not understand or would not reasonably expect, or if you think some Data Subjects would object if you explained it to them. You should also avoid this basis for Processing that could cause harm, unless you are confident there is nevertheless a compelling reason to go ahead which justifies the impact.
- Because this basis is not purpose-specific, it is particularly flexible, and it may be applicable in a wide range of different situations. It can also give you more ongoing control and security over your long-term Processing than Consent, where an individual could withdraw their Consent at any time.
- Legitimate interests are not limited to core activities. This may include Processing of Personal Information to ensure efficient servicing of customers.
- You may have a legitimate interest in transmitting Personal Information to other organisations within your group for administrative purposes. But it does not say this always constitutes a legitimate interest. If you operate within a group of entities and subsidiaries then you may be able to demonstrate that transfers within the group are necessary for a legitimate interest of group administration, but you should identify your specific purpose, show that the Processing of this information is necessary for that purpose, and consider the balancing test.
- While Direct Marketing is recognised as a legitimate interest, you should only rely on legitimate interests for this purpose if you can show that the use case is legitimate and proportionate in a specific instance, has a minimal privacy impact and that your marketing would be reasonably expected by a Data Subject. If the answer is no, then this adds weight against the case for using legitimate interest as a the most appropriate legal ground.

Examples

- You conduct an affordability test which is necessary to ensure that the customer can afford the product.
- Processing is necessary for the prevention, detection investigation or remediation of (suspected) fraud or other misconduct. An example is an insurance company wanting to Process Personal Information to spot fraudulent claims on the basis of legitimate interests. Firstly it considers the purpose test. It is in the company's legitimate business interests to ensure that its customers do not defraud it out of money. However at the same time the company's other customers and the public in general also have a legitimate interest in ensuring that fraud is prevented and detected. Another example is sharing fraud data with other insurers to prevent

fraudulent claims.

- You are a subsidiary of Company A. You do not have a HR department as this function is performed centrally at Company A. You want to rely on legitimate interests as your lawful basis for passing employee data to Company A. You conclude that it is in your legitimate interests to disclose information about leave, sickness, performance etc to your parent company for efficient group HR administration purposes. Processing can be said to be necessary for the sound management of your business.

Objection by the Data Subjects to Processing[15]

9.16. Unless the Processing is required by legislation Data Subjects may object[16] on reasonable grounds to Processing conducted on the following grounds:

9.16.1. protecting the legitimate interests of the Data Subject;

9.16.2. Processing is necessary to pursue your legitimate interests or those of a third party;

9.16.3. Processing is necessary for a public law duty.[17]

9.17. If a Data Subject has objected on reasonable grounds to the Processing of Personal Information for a specific purpose in terms of section 11(3), you may no longer Process the Personal Information.

Guidance notes

- Data Subjects have an absolute right to stop their Personal Information being used for Direct Marketing.
- Once Data Subjects have registered an objection, you should judge whether the objection is reasonable in the particular circumstances. If that is the case, you should end the Processing immediately. You may refuse to comply with the objection, but only if you can prove that the Data Subject's request is unreasonable, and you have a strong reason to continue Processing the Personal Information that overrides the Data Subject's objection.
- Erasure may not be appropriate if you Process the information for other purposes as you need to retain the information for those purposes. For example, when a Data Subject objects to the Processing of their information for Direct Marketing, you should place their details onto an opt-out list to ensure that you continue to comply with their objection. However, you should ensure that the information is clearly marked so that it is not Processed for purposes the Data Subject has objected to and only retain the minimum information you need to give effect to the Data Subject's request not to be contacted.

[15] Section 11(3).
[16] Objections must be in the form of Form 1 to the POPIA Regulations.
[17] Section 11(3).

Example

- Your organisation may consider a request to be unreasonable (e.g. manifestly unfounded or excessive) when it is clear that it has been made with no real purpose except to cause harassment of or disruption to your organisation.

10. COLLECTION DIRECTLY FROM DATA SUBJECTS

10.1. You must collect information directly from the Data Subjects except where POPIA specifically allows collection from other sources.[18]

10.2. Collection from other sources is allowed:[19]

10.2.1. Where the information is contained in or derived from a public record or has deliberately been made public by the Data Subject.

Guidance notes

- "Public domain" is not necessarily a "*public record*".[20]
- Whether information has been deliberately made public will depend on the purpose for which it is published.
- "*Deliberately made public*" is not defined in POPIA, but it clearly assumes a deliberate act by the Data Subject. It is not enough that it is already in the public domain – it must be the person concerned who took the steps that made it public. It refers to the situation where the Data Subject voluntarily and clearly publishes their own Personal Information, such as their name, address, health status, political views, etc., on a public platform, such as a social media site, a blog, or a newspaper. In this case, the Data Subject is considered to have waived their right to privacy and consent for the use of their Personal Information by others. However, this does not mean that anyone can use the Personal Information for any purpose. The Responsible Party still has to comply with the other conditions for lawful Processing, such as having a legitimate interest, respecting the Data Subject's rights, and ensuring data security. The Responsible Party also has to consider the context and the expectations of the Data Subject when they made their information public. For example, if a person posts a photo of themselves on a social media site, they may not expect that their photo will be used for commercial or research purposes without their knowledge or consent. Therefore, the phrase '*deliberately made public by the data subject*' is not a simple or straightforward concept. It requires a careful and case-by-case

[18] Section 12(1).
[19] Section 12(2).
[20] "*Public record*" means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.

analysis of the circumstances and the implications of the Processing. It also implies a responsibility and a respect for the Data Subject's choices and preferences.

- To be manifestly made public, the data must also be realistically accessible to a member of the general public. The question is not whether it is theoretically in the public domain, but whether it is actually publicly available in practice. Disclosures to a limited audience are not necessarily 'deliberately public' for these purposes. In particular, information is not necessarily public just because you have access to it. The question is whether any hypothetical interested member of the public could access this information.
- When you enhance public data with privately obtained Personal Information, the combined data set is no longer public. If the lawful basis Processing privately collected data did not include such enhancement activities – you should not do it.
- Even if the information is publicly available, the Data Subject must still be informed of the use in terms of section 18.

Example

- 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.

10.2.2. Where 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.

10.2.3. Where collection from another source would not prejudice the legitimate interests of the Data Subjects.

Guidance note

- This does not have to be to protect the interests of the Data Subject, only that collection would not prejudice any legitimate interests of the Data Subject.

Examples

- Where information is obtained from a third party to locate/contact a beneficiary under a claim.
- Where information on lives assured or third-party beneficiaries are collected from policyholders.

- You may rely on third party data to verify the Data Subjects' information, for example in an application form. You should list this as a purpose in your Privacy Notice.
- Other examples include joint life insurance and key person or contingent liability insurance.

10.2.4. 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 is collected in the process of independent verification in terms of FICA.
- Information about a customer is collected by an FSP from a product provider to comply with the FAIS advice requirements.

10.2.5. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated.

10.2.6. In the interests of national security.

10.2.7. Where collection from another source is necessary to maintain your legitimate interests or those a third party.

Guidance notes

- You should be able to demonstrate that the collection from a third party is necessary for the purposes of the legitimate interests you have identified. This doesn't mean that it has to be absolutely essential, but it should be a targeted and proportionate way of achieving your purpose.
- 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, you 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) issued under the National Credit Act, No. 34 of 2005 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

- You collect information from data bases through which information about medical impairments and claims are shared to combat fraud, e.g. the applicable industry Life & Claims Register.
- You collect information from credit bureaux for fraud prevention, verifying information or tracing consumers.

10.2.8. Where compliance would prejudice a lawful purpose of the collection.

Guidance note

- Where information has not been collected directly from the Data Subjects because it would prejudice a lawful purpose, you may not use the information so collected for any unrelated purpose.

Example

- Your forensics team collects Personal Information from other sources for purposes of conducting a lawful forensic investigation and notification to the Data Subject would prejudice such an investigation.

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

Example

- It would involve a disproportionate effort to collect data directly from the Data Subject.

Guidance notes

- If you obtain Personal Information from other sources, you should provide Data Subjects with privacy information within a reasonable period of obtaining the information.
- 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. You should accordingly disclose in your Privacy Notices which other sources you may use to collect Personal Information.
- **Buying data from data bases**
  - Where you buy any data base which contains Data Subjects' Personal Information, you should ensure that the Data Subject has Consented that his/her Personal Information is contained on such data base and that it may be shared with you for specific purposes. You should only use the information for those agreed purposes.
  - 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.

- **Leads**
  - If you intend to contact a Data Subject after having obtained a lead you should check if the Data Subject has Consented to his/her information being provided to you and that the information has been lawfully obtained.
  - You should record the details of the person providing the lead, as the Data Subject has the right to know this.
- **Taking out cover for another person**
  - Where someone. takes out cover on the life of another person, or takes out keyman insurance, the insured person's Personal Information may not be collected directly from them. Collection should be justifiable on one of the above bases. e.g. that it does not prejudice the legitimate interests of the Data Subject or that the Data Subject has Consented.

PURPOSE SPECIFICATION

11. COLLECTION FOR A SPECIFIC PURPOSE

11.1. Personal information should be collected for a specific, explicitly defined and lawful purpose related to your functions or activities.[21]

11.2. Steps should be taken in accordance with section 18(1) to ensure that the Data Subject is aware of the purpose of the collection of the information unless the provisions of section 18(4) are applicable.[22]

Guidance notes

- This requirement aims to ensure that you are transparent about your reasons for obtaining Personal Information and that what you will do with the information is in line with the reasonable expectations of the Data Subjects.
- You should be clear about what your purposes for Processing are from the start. 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.
- You should record your purposes as part of your documentation obligations and specify them in your Privacy Notices.

[21] Section 13(1).
[22] Section 13(2).

- You should only use the Personal Information for a new purpose if either this is compatible with your original purpose, you get Consent, or you have a clear obligation or function set out in law.
- Statements of purpose should not be so broad as to make this condition meaningless e.g. "*to serve you better*" or "*for your benefit*".

Examples

- Examples of purposes are:
  - the issue of products, for example a life insurance policy or a participatory interest in a collective investment scheme;
  - the maintenance of a contract;
  - the prevention of crime or fraud;
  - verification of information;
  - communication;
  - debt collection;
  - tracing;
  - the assessment and processing of claims;
  - compliance with statutory or regulatory obligations or other obligations imposed by law;
  - providing marketing information to Data Subjects who requested to receive such information.

12. RECORD RETENTION

12.1. Subject to the provisions below, 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:[23]

Guidance note

- For a retention period to take effect, a trigger event should be applied in the lifecycle of the information and the information should be destroyed, de-identified or deleted within a certain period thereafter. This point varies according to the type of information.

Examples

- Examples of trigger events are folder closures, termination of a contract, a claim

[23] Section 14(1).

event, reaching a certain age, date of last correspondence or disinvestment/withdrawal dates.

12.1.1. Retention of the record is required or authorised by law.

Guidance notes

- In determining appropriate retention periods, regard should be had to statutory retention periods and obligations imposed on you. Various statutes prescribe the minimum period for which records must be kept (see **Examples** below).
- Where different legislation refers to the retention of the same records/information, you should consider adhering to the most stringent of the legislative requirements.
- Regard should be had to 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 should be considered.
- For more guidance on statutory retention periods, see the SAICA Guide on the Retention of Records.

Examples

- Sections 22, 22A and 23 of FICA and Guidance Note 7 provide that records must be kept for at least 5 years from the date on which the business relationship is terminated or the transaction is concluded.
- Section 29 of FICA provides in respect of suspicious and unusual transactions that records must be kept at least 5 years from the date on which the report was submitted to the FIC.
- Section 24 of the Companies Act, No. 71 of 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.
- Regard may be had to the Prescription Act, No. 69 of 1969 to determine periods within which claims will prescribe.
- Section 74 of CISCA provides that accounting records must be kept of at least 5 years from the date of the latest entry therein.
- Section 26 of the Consumer Protection Act of 2008 provides that a person who conducts a promotional competition must retain related information for a period of 3 years.

12.1.2. You reasonably require the record for lawful purposes related to your functions or activities.

Guidance notes

- You should consider whether you need to keep information to defend possible future legal claims. However, you could still delete information that could not possibly be relevant to such a claim. Unless there is some other reason for keeping it, Personal Information should be deleted when such a claim could no longer arise.
- You should consider any legal or regulatory requirements. There are various legal requirements and professional guidelines about keeping certain kinds of records – such as information needed for income tax, audit and reporting purpose. If you keep Personal Information to comply with a requirement like this, you will not be considered to have kept the information for longer than necessary.
- You should not use this exception as a blanket justification to hold all Personal Information on the off chance that it may be useful in the future, but should constantly weigh up the rights of the Data Subjects to the privacy of their information versus your business's need to retain the information.
- You should consider whether you need to keep a record of a relationship with the Data Subject once that relationship ends. You may not need to delete all Personal Information when the relationship ends. You may need to keep some information so that you can confirm that the relationship existed – and that it has ended – as well as some of its details.
- You should use best endeavours to appropriately safeguard the information from being used for any other purpose.

Examples

- You may need to keep some Personal Information about a previous customer so that you can deal with any complaints the customer might make about the services they provided.
- Where Data Subjects apply for but do not subsequently proceed with a transaction, or it is declined, you may keep their details on file for a limited period to facilitate a subsequent application, enquiries or a check against non-disclosure.
- If you receive a notice from a former customer requiring you to stop Processing the customer's Personal Information for Direct Marketing, it is appropriate to retain enough information about the former customer for you to stop including the person in future Direct Marketing activities.
- You may need to keep Personal Information so that you can defend possible future legal claims. Statutory prescription periods may be useful to determine retention periods.
- You may need to keep Personal Information for the prevention of fraud, money laundering, terrorist-financing, corruption, tax evasion and other illicit financial crime purposes. 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.

12.1.3. Retention of the record is required by a contract between the parties thereto.

12.1.4. The Data Subject or a Competent Person, where the Data Subject is a Child, has Consented to the retention of the record.

12.2. Records of Personal Information may be retained for periods in excess of those contemplated above for historical, statistical or research purposes if you have established appropriate safeguards against the records being used for any other purposes.[24]

12.3. If you have 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 if there is no law, for a period which will afford the Data Subjects a reasonable opportunity to request access to the record.[25]

[24] Section 14(2).
[25] Section 14(3).

12.4. Once you may no longer hold Personal Information, you must destroy, delete or de-identify[26] the information as soon as reasonably possible.[27]

Guidance notes

- Destruction or deletion should be such that any reconstruction is prevented.
- It is good practice to keep an audit trail of deletion/destruction of Personal Information.
- In the case of paper files held by organisations, deletion is straightforward and can be effected by, for example, shredding or incineration. It is more complicated when data is held electronically, as "deleted" data may still exist on an organisation's systems. Where information has been deleted, but where it still exists in the "electronic ether", such data will not be "live data", and therefore data protection compliance issues will not apply to the data, as long as the Responsible Party does not intend to use or access the data again. An analogy can be drawn with a bag of shredded paper files-it would be possible to reconstitute the information from the shredded paper, but it would be extremely difficult, and it is unlikely that the organisation would have any intention of doing so.
- It is possible for a Responsible Party to put undeleted data "beyond use" if the Responsible Party:
  - is not able, or will not attempt, to use the Personal Information to inform any decision in respect of a Data Subject or in a manner that affects the Data Subject in any way;
  - does not give any other organisation access to the Personal Information;
  - puts appropriate security measures in place in relation to the Personal Information; and
  - commits to permanent deletion of the Personal Information if and when it becomes possible.
- If Personal Information is stored offline, this should reduce its availability and the risk of misuse or mistake. However, you are still Processing Personal Information. You should only store it offline (rather than delete it) if you can still justify holding it. You should be prepared to respond to subject access requests for Personal Information stored offline, and you must still comply with all the other principles and rights.

12.5. You must restrict Processing of Personal Information if:[28]

12.5.1. Its accuracy is contested by the Data Subject, for a period enabling you to verify the accuracy of the information.

---

[26] "*de-identify*", is defined in POPIA, in relation to Personal Information of a Data Subject, to delete any information that—
(a) identifies the Data Subject;
(b) can be used or manipulated by a reasonably foreseeable method to identify the Data Subject; or
(c) can be linked by a reasonably foreseeable method to other information that identifies the Data Subject.
[27] Section 14(4).
[28] Section 14(6).

Example

- A Data Subject believes that information held about them is inaccurate. They repeatedly request its correction but you have previously investigated and verified that it is accurate. The Data Subject continues to make requests along with unsubstantiated claims against you as the Responsible Party. You refuse the most recent request because it is manifestly unfounded and you notify the Data Subject of this.

12.5.2. You no longer need the Personal Information for achieving the purpose for which the information was collected or subsequently Processed, but it has to be maintained for purposes of proof.

12.5.3. The Processing is unlawful and the Data Subject opposes its destruction or deletion and requests the restriction of its use instead.

12.5.4. The Data Subject requests to transmit the Personal Information into another automated processing system.

12.6. Personal Information referred to in paragraph 0 may, with the exception of storage, only be Processed for purposes 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.

General

Guidance notes

- POPIA does not set specific time limits for different types of information. This is up to you and will depend on how long you need the information for your specified purposes.
- Ensuring that you erase or de-identify Personal Information when you no longer need it will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. Apart from helping you to comply with the minimisation and accuracy conditions, this also reduces the risk that you will use such information in error – to the detriment of all concerned.
- Personal Information held for too long will, by definition, be unnecessary. You are unlikely to have a lawful basis for retention.
- 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 requirements in section 14, need to be interpreted in a manner that gives effect to this purpose. You should take a proportionate approach, balancing your needs with the impact of retention on the Data Subject's privacy.
- It is recommended that you proceed cautiously prior to launching extensive record destruction programmes and 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.

- If you share Personal Information with other organisations, you should agree between you what happens once you no longer need to share the information. In some cases, it may be best to return the shared information to the organisation that supplied it without keeping a copy. In other cases, all of the organisations involved should delete their copies of the Personal Information.

How long should records be kept for?

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.
- It is recommended that you:
  - consider what Personal Information you hold and for which purposes;
  - determine the length of time you would need to hold the information in order to fulfil those purposes;
  - consider whether there are any lawful bases in terms of section 14 to hold the information for longer periods than to achieve the stated purposes and how low you would need to/may hold the information on those bases.
- Determining retention periods is ultimately a matter of risk management. You should conduct your 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 you keep to these retention periods.

Data retention policies

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

Guidance notes

- Retention policies or retention schedules list the types of record or information you hold, what you use it for, and how long you intend to keep it. They help you establish and document standard retention periods for different categories of Personal Information.
- To comply with documentation requirements (section 17), you should establish and document standard retention periods for different categories of information you hold wherever possible. It is also suggested to have a system for ensuring that your organisation keeps to these retention periods in practice, and for reviewing retention at appropriate intervals.

- Data retention policies should, *inter alia,* deal with:
  - best practice for the key type of records identified;
  - the different purposes for which you hold 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.
- There is a tangled web of potentially relevant laws so you should take care in drafting your policy.

FURTHER PROCESSING LIMITATION

13. COMPATIBLE PURPOSE

Further Processing must be compatible with original purpose of collection

13.1. You may process Personal Information only if such Processing is compatible with the original purpose for which it was collected.

13.2. To assess whether further Processing is compatible with the purpose of collection, you must take account of:[29]

13.2.1. the relationship between the purpose of the intended further Processing and the purpose for which the information has been collected;

13.2.2. the nature of the information concerned;

13.2.3. the consequences of the intended further Processing for the Data Subject;

13.2.4. the manner in which the information has been collected; and

13.2.5. any contractual rights and obligations between the parties.

Guidance notes

[29] Section 25(2).

- You should do a compatibility assessment to decide whether a new purpose is compatible with your original purpose. The assessment should take into account:
  - any link between your original purpose and the new purpose;
  - the context in which you originally collected the Personal Information – in particular, your relationship with the Data Subject and what they would reasonably expect;
  - the nature of the Personal Information – e.g. is it particularly sensitive;
  - the possible consequences for Data Subjects of the new Processing; and
  - whether there are appropriate safeguards – e.g. encryption or anonymization.
- As a general rule, if the new purpose is either very different from the original purpose, would be unexpected, or would have an unjustified impact on the Data Subject, it is likely to be incompatible with your original purpose. In practice, you are likely to need to ask for specific Consent to use or disclose information for this type of purpose.

Examples

- Examples of further Processing by Responsible Parties include, but are not limited to:
  - the Direct Marketing of products or services to existing and potential customers;
  - direct marketing by product suppliers to intermediaries who place business with them via third-party platforms;
  - cross selling (to the extent not specified in the original purpose); and
  - profiling.

13.3. The further Processing of Personal Information is not incompatible with the purpose of collection if:[30]

13.3.1. The Data Subject or a Competent Person, where the Data Subject is a Child, has Consented to the further Processing of the information.

Example

- You disclose Personal Information to persons appropriately authorised to act on behalf of the Data Subjects (i.e. appointed by the Data Subject or acting in the place of the Data Subject), such as curators, executors or agents.

[30] Section 15(3).

13.3.2. The information is available in or derived from a public record or has deliberately been made public by the Data Subject.

13.3.3. Further Processing is necessary:

13.3.3.1. to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;

13.3.3.2. 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, No. 34 of 1997.

Examples

- You have to report a cash transaction above the prescribed threshold to the FIC.
- You provide information requested lawfully by the Financial Sector Conduct Authority, the Prudential Authority, SARS, the FIC or any other applicable regulatory body.

13.3.3.3. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated.

13.3.3.4. In the interests of national security.

13.3.4. The further Processing of the information is necessary to prevent or mitigate a serious and imminent threat to:

13.3.4.1. public health or public safety; or

13.3.4.2. the life or health of the Data Subject or another individual.

13.3.5. The information is used for historical, statistical or research purposes and you ensure that the further Processing is carried out solely for such purposes and will not be published in an identifiable form.

13.3.6. The further Processing of the information is in accordance with an exemption granted under section 37 of POPIA.

Example

- A GP discloses his patient list to an insurance company so that it can offer disability cover to patients. Disclosing the information for this purpose would be incompatible with the purposes for which it was obtained.

INFORMATION QUALITY AND DOCUMENTS

14. INFORMATION QUALITY

14.1. You 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.[31]

Guidance notes

- Whether or not to keep Personal Information up to date will depend on what the information is used for. If the information is used for a purpose that relies on it remaining current, it should be kept up to date. You should, for example, update your records for existing customers' changes of contact details so that you can communicate with them. In other cases, it will be obvious that you do not need to update information. You would not need to update Personal Information if this would defeat the purpose of the Processing. For example, if you hold Personal Information only for statistical, historical or other research reasons, updating the data might defeat that purpose.
- Ensuring information quality should be an ongoing process.
- You should request your Data Subjects to keep their information up to date and make it easy for Data Subjects to do so.
- You should conduct regular data quality reviews of records containing Personal Information to make sure they are accurate, adequate and not excessive.

15. DOCUMENTS

15.1. You must maintain the documentation of all Processing operations under your responsibility as referred to in section 51 of PAIA, in the form of a PAIA manual.[32]

Guidance note

- Section 51 of PAIA has been extensively amended by POPIA. The PAIA Manual must now include information that relates to the Processing of Personal Information by a private body.

OPENNESS

16. NOTIFICATION TO THE DATA SUBJECTS

[31] Section 16.
[32] Section 17.

16.1. When Personal Information is collected, you must take reasonably practicable steps to ensure that the Data Subjects are aware of:[33]

16.1.1. the information being collected and where the information is not collected from the Data Subjects, the source from which it is collected;

16.1.2. your name and address;

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

16.1.4. whether or not the supply of the information by the Data Subjects is voluntary or mandatory;

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

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

16.1.7. the fact that, where applicable, you intend 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 organisation;

16.1.8. any further information, such as:

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

16.1.8.2. nature or category of the information;

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

16.1.8.4. existence of the right to object to the Processing of Personal Information;

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

16.1.9. any further information which is necessary under the specific circumstances to ensure reasonable Processing.

16.2. It is not necessary for you to comply with the above notification requirements where:

16.2.1. the Data Subject has provided Consent for the non-compliance;

16.2.2. non-compliance would not prejudice the legitimate interests of the Data Subject;

---

[33] Section 18(1).

16.2.3. non-compliance is necessary:

16.2.3.1. to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

16.2.3.2. to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;

16.2.3.3. for the conduct of proceedings in any court or tribunal; or

16.2.3.4. in the interests of national security;

16.2.4. compliance would prejudice a lawful purpose of the collection;

16.2.5. compliance is not reasonably practicable in the circumstances of the particular case; or

16.2.6. the information will—

16.2.6.1. not be used in a form in which the Data Subject may be identified; or

16.2.6.2. be used for historical, statistical or research purposes.

Guidance notes

- You should be transparent about your reasons for obtaining Personal Information and should ensure that what you do with the information is in line with the reasonable expectations of the Data Subjects.
- You should ensure that your organisation has a Privacy Notice which contains all the prescribed information.
- You should proactively make Data Subjects aware of privacy information and have a free, easy way to access it.
- You should write privacy information in clear and plain language that the intended audience can understand, and offer it in accessible formats if required.
- When dealing with potential customers telephonically, you should refer them to your organisation's Privacy Notice.
- You do not have to restrict Privacy Notices to a single document or page on your websites. Other ways to display privacy information include:
    - **A layered approach** – short notices containing key privacy information that have additional layers of more detailed information;
    - **Dashboards** – preference management tools that inform people how you use their information and allow them to manage what happens with it;
    - **Just-in-time notices** – relevant and focused privacy information delivered at the time you collect individual pieces of information, providing a brief message explaining how the information they are about to provide will be used;

- **Icons** – small, meaningful, symbols that indicate the existence of a particular type of information Processing;
- **Mobile and smart device functionalities** – including pop-ups, voice alerts and mobile device gestures.

- You should consider whether it is in the customer's interest to provide more detailed information about certain Processing referred to in your Privacy Notice. This could be done by following a layered approach.

16.3. If information is collected from the Data Subjects, you must inform the Data Subjects prior to the collection, unless the Data Subjects are already aware of the information.[34]

16.4. 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

- Data Subjects should receive privacy information when their data is collected (e.g. when they fill in a form) or by observation (e.g. when using CCTV or people are tracked online).
- If information is collected from another source, it is recommended that Data Subjects be informed within 1 month of collection.

Example

- Where Data Subjects are third party claimants who would not otherwise have received a notice, an appropriate Privacy Notice in terms of section 18 must be made available at a suitable point in the business process, e.g. a claims procedure document.

16.5. It is not always necessary to notify the Data Subjects in terms of section 18(1), namely where:

16.5.1. The Data Subject or a Competent Person where the Data Subject is a Child has Consented to the non-notification.

16.5.2. Non-compliance won't prejudice the legitimate interests of the Data Subjects.

Example

- You Process Personal Information in order to trace a beneficiary.

[34] Section 18(2).

16.5.3. Non-compliance is necessary to avoid prejudice to the maintenance of the law.

Example

- You investigate an incidence of fraud.

16.5.4. It is necessary for the conduct of court or tribunal proceedings.

16.5.5. Compliance would prejudice a lawful purpose of the collection.

16.5.6. It is not reasonably practicable in the circumstances of the case.

Guidance note

- Where notification before collection is not practicable or reasonable, you should at least try to notify before using or disclosing the information.

PART 4: SECURITY SAFEGUARDS

17. SECURITY MEASURES ON INTEGRITY OF PERSONAL INFORMATION

17.1. You must secure the integrity and confidentiality of Personal Information in your possession or under your control by taking appropriate, reasonable technical and organisational measures to prevent:[35]

17.1.1. loss of, damage to or unauthorised destruction of Personal Information; and

17.1.2. unlawful access to or Processing of Personal Information.

17.2. In order to give effect to the above obligation, you must take reasonable measures to:

17.2.1. identify all reasonably foreseeable internal and external risks to Personal Information;

17.2.2. establish and maintain appropriate safeguards against risks identified;

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

17.2.4. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.[36]

[35] Section 19(1).
[36] Section 19(2).

17.3. The technical and organisational measures taken must ensure an appropriate level of security.[37]

17.4. You should also have due regard to generally accepted information security practices and procedures which may apply to you generally or be required in terms of industry or professional rules and regulation.[38]

Guidance notes

- There is no "one size fits all" solution to information security. The security measures that are appropriate for you will depend on the circumstances, so you should adopt a proportionate risk-based approach to deciding what level of security you need.
- You should undertake an analysis of the risks presented by your Processing, and use this to assess the appropriate level of security you need to put in place.
- Appropriate security means that you should take into account include:
  - things like risk analysis, organisational policies, and physical and technical measures;
  - the risks involved in Processing and the nature of the information to be protected. The more sensitive the information, the higher the applied security should be;
  - the security outcomes you want to achieve. The outcomes intend to provide a common set of expectations that you can meet, either through following existing guidance, using particular services or, if you are sufficiently competent, development of your own bespoke approach;
  - the state of the art and cost of the implementation measures to take - but they should be appropriate both to your circumstances and the risk your Processing poses;
  - the measures that would enable you to restore access and availability to Personal Information in a timely manner in the event of a physical or technical incident.
- It is recommended that you have an information security policy (or equivalent) and take steps to make sure the policy is implemented.
- You should consider the security outcomes you want to achieve, e.g. with regards to:
  - managing security risks: governance, risk management, asset management, Operators and the supply chain;
  - protection against cyberattacks service protection policies and processes, identification and access control, data security, system security and staff training and awareness;

[37] Section 19(3).
[38] Section 19(4).

- detecting security events and security monitoring;
- minimising impact, such as response and recovery planning and improvements.

- Other good practices include:
  - designing and organising your security to fit the nature of the Personal Information you hold and the harm which may result from a security breach;
  - being clear who in the organisation is responsible for ensuring information security;
  - making sure you have the right physical and technical security, backed up by robust policies and procedures and reliable well-trained staff; and
  - being ready to respond to any breach of security swiftly and effectively.
- You should also, as part of good practice, be in a position to provide evidence of reasonable steps taken to secure Personal Information.
- You should have regard to internationally accepted standards for privacy information management which focus holistically on preventative, detective and corrective controls. Two of the most widely known frameworks for information security are the Cybersecurity Framework, created by the National Institute of Standards and Technology (NIST); and the ISO 27001 standard, created by the International Organization for Standardization (ISO).

Examples

- Appropriate technical and organisational measures for safeguarding Personal Information include:
  - agreeing appropriate confidentiality undertakings with employees and contractors;
  - checking periodically whether systems require adaptation, for example due to technological developments;
  - ensuring that staff understand the importance of protecting Personal Information and are trained on how to properly deal with Personal Information;
  - encrypting all removable media used for taking Personal Information offsite;
  - using passwords to protect Personal Information; and
  - securing the transmission of Personal Information.

18. RESPONSIBLE PARTIES AND OPERATORS

Who is a Responsible Party?

18.1. A Responsible Party is defined in POPIA as a person who 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.

Guidance note

- You are most likely to be a Responsible Party if:
  - you decide to collect or Process the Personal Information;
  - you decide what the purpose or outcome of the Processing is to be;
  - you decide what Personal Information should be collected;
  - you decide which Data Subjects to collect Personal Information about;
  - you obtain a commercial gain or other benefit from the Processing, except for any payment for services from another Responsible Party;
  - you are Processing the Personal Information as a result of a contract between yourself and the Data Subject;
  - 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;
  - you have a direct relationship with the Data Subjects;
  - you have complete autonomy as to how the Personal Information is Processed;
  - you have appointed the Operators to Process the Personal Information on your behalf.

Joint Responsible Parties

18.2. Responsible Parties can determine the purposes and means of Processing alone or jointly with others – as a joint Responsible Party.

Guidance notes

- If two or more Responsible Parties jointly determine the purposes and means of the Processing of the same Personal Information, they are joint Responsible Parties. However, Responsible Parties will not be joint Responsible Parties if they are Processing the same information for different purposes.
- You are most likely to be a joint Responsible Party if:
  - you have a common objective with others regarding the Processing;
  - you are Processing the Personal Information for the same purpose as another Responsible Party;
  - you are using the same set of Personal Information (e.g. one database) for this Processing as another Responsible Party;
  - you have designed this process with another Responsible Party.
  - you have common information management rules with another Responsible Party.

Examples

- Your organisation contracts a market-research company to carry out some research. Your brief specifies your budget and that you require a satisfaction survey of your main retail services based on the views of a sample of its customers. You leave it to the research company to determine sample sizes, interview methods and presentation of results. The research company is Processing Personal Information on your organisation's behalf, but it is also determining the information that is collected (what to ask your customers) and the manner in which the Processing (the survey) will be carried out. It has the freedom to decide such matters as which customers to select for interview, what form the interview should take, what information to collect from customers and how to present the results. This means the market-research company is a joint Responsible Party with your organisation regarding the Processing of Personal Information to carry out the survey, even though your organisation retains overall control of the information because you commission the research and determine the purpose the information will be used for.
- An insurance company that teams up with a nutrition company to host a co-branded promotional event. The companies decide to run a prize draw at the event. They invite attendees to participate in the prize draw by entering their name and address into their prize draw system at the event. After the event, the companies post out the prizes to the winners. They do not use the Personal Information for any other purposes. The companies will be joint Responsible Parties of the Personal Information processed in connection with the prize draw, because they both decided the purposes and means of the Processing.

Operators

18.3. An "*operator*" is defined in POPIA as "*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*".

Guidance notes

- You will not always process Personal Information yourself, but may have the Processing carried out by an Operator on your behalf.
- Operators act on your behalf as a Responsible Party and under your authority. In doing so, they serve your interests rather than their own.
- Although an Operator may make its own day-to-day operational decisions, it may only Process Personal Information in line with your instructions, unless it is required to do otherwise by law.
- If an Operator acts without your instructions in such a way that it determines the purpose and means of Processing, including to comply with a statutory obligation, it will be a Responsible Party in respect of that Processing and will have the same liability as a Responsible Party.
- You 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.

- You do not need the Consent of Data Subjects or any other lawful basis for Processing in order to share Personal Information with your chosen Operator(s). However, you should stipulate in your Privacy Notice which types/categories of Operators you use.
- Whether you are a Responsible Party or Operator depends on a number of issues. The key question is – who determines the purposes for which the information is Processed and the means of Processing? Organisations that determine the purposes and means of Processing will be Responsible Parties regardless of how they are described in any contract about Processing services.
- You are likely to be an Operator if:
    - you are following instructions from someone else regarding the Processing of Personal Information;
    - you are given the Personal Information by a customer or similar third party, or told what information to collect;
    - you do not decide to collect Personal Information;
    - you do not decide what Personal Information should be collected;
    - you do not decide the lawful basis for the use of that information;
    - you do not decide what purpose or purposes the information will be used for.
    - you do not decide whether to disclose the information, or to whom;
    - you do not decide how long to retain the information;
    - you may make some decisions on how information is Processed, but implement these decisions under a contract with someone else;
    - you are not interested in the end result of the Processing.
- However, within the terms of its contract with the Responsible Party, an Operator may decide:
    - what IT systems or other methods to use to collect Personal Information;
    - how to store the Personal Information;
    - the details of the security measures to protect the Personal Information;
    - how it will transfer the Personal Information from one organisation to another;
    - how it will retrieve Personal Information about certain Data Subjects;
    - how it will ensure it adheres to a retention schedule; and
    - how it will delete or dispose of the information.
- **Can you be both a Responsible Party and an Operator of Personal Information?**
    - Yes. If you are an Operator that provides services to other Responsible Parties, you are very likely to be a Responsible Party for some Personal Information and an Operator for other Personal Information. For example, you will have your own employees so you will be a Responsible Party regarding your employees'

Personal Information. However, you cannot be both a Responsible Party and an Operator for the same Processing activity.

- In some cases, you could be a Responsible Party and an Operator of the same Personal Information – but only if you are Processing it for different purposes. You may be Processing some Personal Information as an Operator for the Responsible Party's purposes and only on its instruction, but also Process that same Personal Information for your own separate purposes. In particular, if you are an Operator, you should remember that as soon as you Process Personal Information outside your Responsible Party's instructions, you will be acting as a Responsible Party in your own right for that element of your Processing.

- You should carefully consider your relationships with independent brokers. As long as the broker is Processing Personal Information as part of its own business of rendering financial services, the broker should generally not be an Operator, but a Responsible party in its own right. However, if you outsource other client services to the broker, the broker may very well be an Operator for which you will be responsible.

Examples

- You hire an IT services firm to store archived information on your behalf. You will still control how and why the information is used and determine its retention period. In reality the IT services firm will use a great deal of its own technical expertise and professional judgement to decide how best to store the information in a safe and accessible way. However, despite this freedom to take technical decisions, the IT firm is still not a Responsible Party in respect of your data – it is an Operator. This is because you retain exclusive control over the purpose for which the information is Processed, if not exclusively over the manner in which the Processing takes place.
- You have a broker contract with a financial service provider firm, in terms whereof the firm procures business for your organisation. To the extent that the broker collects or otherwise Processes Personal Information of clients on your behalf, it will be regarded as your Operator, even if the broker uses the same information in order to render financial services to the client, for which purposes it will be a Responsible Party in its own right.
- An insurer is sending envelopes containing customer information to health providers for underwriting assessment purposes and contracts a delivery service to deliver them. The delivery service is not Processing the Personal Information contained in those envelopes. Although it is in physical possession of the envelopes, it has no idea what the envelopes contain and may not open them to access the content. For data protection purposes, the delivery service does not 'Process' any Personal Information contained within those envelopes.
- Employer A hires accounting firm C to carry out audits of their bookkeeping and therefore transfers information about financial transactions (including Personal Information) to C. C Processes this information without detailed instructions from A. C decides itself, in accordance with legal provisions regulating the tasks of the auditing activities carried out by C, that the information it collects will only be Processed for the purpose of auditing A and it determines what information it

needs to have, which categories of persons that need to be registered, how long the information shall be kept and what technical means to use. Under these circumstances, C is to be regarded as a Responsible Party of its own when performing its auditing services for A. However, this assessment may be different depending on the level of instructions from A. In a situation where the law does not lay down specific obligations for the accounting firm and the client company provides very detailed instructions on the Processing, the accounting firm would indeed be acting as an Operator. A distinction could be made between a situation where the Processing is - in accordance with the laws regulating this profession - done as part of the accounting firm's core activity and where the Processing is a more limited, ancillary task that is carried out as part of the client company's activity.

- An insurer outsources its client support to a company who provides a call centre in order to help the insurer's clients with their questions. The client support service means that the call centre has to have access to the insurer's client data bases. The call centre can only access data in order to provide the support that the insurer has procured and they cannot Process data for any other purposes than the ones stated by the insurer. The call centre is to be seen as an Operator.
- A large cloud storage provider offers its customers the ability to store large volumes of Personal Information. The service is completely standardised, with customers having little or no ability to customise the service. The terms of the contract are determined and drawn up unilaterally by the cloud service provider, provided to the customer on a "take it or leave it basis". Company X decides to make use of the cloud provider to store personal information concerning its customers. Company X will still be considered a Responsible Party, given its decision to make use of this particular cloud service provider in order to Process Personal Information for its purposes. Insofar as the cloud service provider does not Process the Personal Information for its own purposes and stores the data solely on behalf of its customers and in accordance with instructions, the service provider will be considered as an Operator.
- In performing its services to contracted financial services providers, Astute Processes Personal Information on the financial services providers' behalf, such as providing consolidated client portfolio information. In this capacity, Astute is acting as an Operator.

Requirements for Operators

18.4. You (as a Responsible Party) must, in terms of a yourself and the Operator, ensure that the Operator which Processes Personal Information on your behalf establishes and maintains the security measures referred to in section 19.[39]

Guidance notes

- You should identify all your Operators and ensure that appropriate written agreements are in place, ensuring at least that the Operator will apply adequate

[39] Section 21(1).

security and confidentiality measures which will not put you at risk of breaching your obligations under POPIA.

- Operator agreements should, at a minimum, contain the following details:
  - the subject matter, duration, nature and purpose of the Processing;
  - the type of Personal Information being Processed;
  - the categories of Data Subjects whose Personal Information is being Processed; and
  - the obligations and rights of the Responsible Party.
- It is also good practice for an Operator agreement to contain the following provisions:
  - that the Operator will only Process Personal Information received from the Responsible Party on documented instructions of the Responsible Party (unless required by law to Process Personal Information without such instructions) including in respect of international data transfers;
  - that the Operator ensures that any person(s) Processing Personal Information is subject to a duty of confidentiality;
  - that the Operator takes all measures required pursuant to section 19 (Security of Processing), including but not limited to implementing appropriate technical and organisational measures to protect Personal Information received from the Responsible Party;
  - that the Operator obtains either a prior specific authorisation or general written authorisation for any sub-processors the Operator may engage to Process the Personal Information received from the Responsible Party;
  - that any sub-processors engaged by the Operator are subject to the same data protection obligations as the Operator and that the Operator remains directly liable to the Responsible Party for the performance of a sub-processor's data protection obligations;
  - that the Operator assists the Responsible Party by appropriate technical and organisational measures to respond to Data Subject rights' requests under POPIA;
  - that the Operator assists the Responsible Party to ensure compliance with obligations under POPIA in relation to security of data Processing, notification of data breaches and data protection impact assessments;
  - that, at the end of the data Processing by the Operator and on the Responsible Party's instruction, the Operator deletes or returns the Personal Information received from the Responsible Party; and
  - that the Operator makes available to the Responsible Party all information necessary to demonstrate compliance with POPIA and that the Operator allows for and contributes to audits conducted by the Responsible Party or a third party on the Responsible Party's behalf.
- It is important to bear in mind that you, as the Responsible Party, remain responsible

for any Processing conducted by an Operator on your behalf.

19. NOTIFICATION OF SECURITY COMPROMISES

19.1. Where there are reasonable grounds to believe that Personal Information has been accessed or acquired by an unauthorised person, you 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 your information system.[40]

19.2. You may only delay notification of the Data Subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.[41]

19.3. The notification to Regulator must be in writing and must be communicated to the Data Subject by mail, email or placed on a prominent position on your website, published in the media or as may be otherwise directed by the Regulator. [42]

19.4. The notification must provide sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise, including a description of the possible consequences of the security compromise, a description of the measures you intend to take or have taken to address the security compromise, a recommendation about the measures to be taken by the Data Subject to mitigate the possible adverse effects of the security compromise and, if known, the identity of the unauthorised person who has accessed the information.[43]

19.5. An Operator must 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.[44]

Guidance notes

- A Personal Information breach means a breach of security leading to the accidental or unlawful unauthorised disclosure of, or access to, Personal Information.
- The intention of breach reporting and notification to the Data Subject is to prevent harm to Data Subjects.

[40] Section 22(1).
[41] Section 22(3).
[42] Section 22(5).
[43] Section 22(5).
[44] Section 21(2).

- "*Reasonable grounds to believe*" means the facts within a person within your organisation's knowledge would satisfy a reasonable person standing in the shoes of that person that there is reason to believe that a security compromise has taken place.
- Your Operator agreements should provide that the Operator informs you as soon as reasonably possible of any security compromises.

Examples

- You detect an intrusion into your network and become aware that files containing Personal Information have been accessed, but you don't know how the attacker gained entry, to what extent that data was accessed, or whether the attacker also copied the data from your system. You notify the Regulator as soon as reasonably possible of becoming aware of the breach, explaining that you don't yet have all the relevant details, but that you expect to have the results of your investigation within a few days. Once your investigation uncovers details about the incident, you give the Regulator more information about the breach without delay.
- An employee in your claims department emailed a vulnerable new client's file in error to a colleague in a different department. The colleague who received the file immediately deleted the email and informed the sender of the error. The file contained information about the client's mental health and reasons for claim. The recipient correctly deleted the email and informed the sender. As a result, it is very unlikely that there would be any unauthorised access of the information by a third party and therefore there is no legal obligation to report the breach to the Regulator or inform the affected Data Subject.
- 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 is unlikely to have been accessed or acquired by any unauthorized person;
    - 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 is unlikely to have been accessed or acquired by any unauthorized person.

  You accordingly don't have to report the incident to the Regulator or notify the Data Subjects.
- An employee lost his briefcase, containing work on an unencrypted laptop and unredacted paper files relating to a sensitive court case – including information on criminal convictions and health information. Initially, the employee told his manager that he believed the laptop was encrypted and the paper files were redacted. The manager reported the incident to the IT department, who remotely wiped the laptop. At that point, you did not report the breach to the Regulator as you believed there was little or no risk to Data Subjects, though you did record the incident on your breach log. After being informed by the IT department that the laptop was unencrypted, and after the employee discovered the paper files had

not been redacted, you identified the possibility unauthorised access and you correctly reported the breach to the Regulator and informed the Data Subjects. You updated your internal breach log to reflect the new information and documented the developing situation, including the way the breach changed from being not reportable to reportable.

PART 5: DATA SUBJECTS' PARTICIPATION

20. ACCESS TO PERSONAL INFORMATION

20.1. A Data Subject, having provided adequate proof of identity, has the right to:[45]

20.1.1. request you to confirm, free of charge, whether or not you hold Personal Information about the Data Subject; and

20.1.2. request from you the record or a description of the Personal Information about the Data Subject held by you, 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.

20.2. If, in response, Personal Information is communicated to a Data Subject, the Data Subject must be advised of the right in terms of section 24 to request the correction of information.[46]

20.3. You may or should refuse to disclose any information requested to which the grounds for refusal of access to records set out in the applicable sections of Chapter 4 of Part 2 and Chapter 4 of Part 3 of PAIA apply. The provisions of sections 30 and 61 of PAIA are applicable in respect of access to health or other records.[47]

20.4. The provisions of sections 18 and 53 of PAIA apply to requests made in terms of section 23.[48]

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, for example where the request is for a large number of records or requires a collation of records from various

[45] Section 23(1).
[46] Section 23(2).
[47] Section 23(4).
[48] Section 25.

different divisions or locations.

- PAIA lists the following 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 your trade secrets or confidential information;
  - 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.
- If you're dealing with a complex or particularly large data access request, you could explain that you'll send out information in batches and provide a timeframe for this.
- You should explain exemptions if they apply. While a customer may not be happy, providing an explanation of why information has not been provided can help them understand your decision. The same can be said for any information you redact. Keep a record of your decision making so that you can share it with the Regulator if questioned.

21. CORRECTION AND DESTRUCTION OF PERSONAL INFORMATION

21.1. Data subjects are allowed to request[49] you to:

21.1.1. correct their Personal Information if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

21.1.2. destroy a record of Personal Information which you may no longer keep in terms of POPIA.[50]

21.2. Upon receipt of such a request, you must:

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

[49] Requests must be made in the form of Form 2 of the POPIA Regulations.
[50] Section 24(1).

21.2.2. notify the Data Subjects of the actions taken and provide evidence in support thereof or notify the Data Subjects if you refuse to make the correction; and

21.2.3. where you are unable to accede to the Data Subjects' request, and where the Data Subjects so request, flag the information as having been challenged.[51]

21.3. If a correction of Personal Information will have an impact on decisions which have been or will be made about the Data Subjects, you must, if reasonably practicable, inform all third parties to whom the information has previously been disclosed of the change.[52]

Guidance notes

- The Data Subject's right to rectification right has close links to the accuracy condition. However, although you may have already taken steps to ensure that the Personal Information was accurate when you obtained it, this right imposes a specific obligation to reconsider the accuracy upon request.
- If you receive a request for rectification, you should take reasonable steps to satisfy yourself that the Personal Information is accurate and to rectify the information if necessary. You should take into account the arguments and evidence provided by the Data Subject. You may also take into account any steps you have already taken to verify the accuracy of the information prior to the challenge by the Data Subject.
- It is complex if the information in question records an opinion. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified.
- Section 24(2) contemplates refusal to rectify. You should let the Data Subject know if you are satisfied that the Personal Information is accurate, and tell them that you will not be amending the information. You should explain your decision, and inform them of their right to make a complaint to the Regulator or another supervisory authority. It is also good practice to place a note on your system indicating that the Data Subject challenges the accuracy of the information and their reasons for doing so.
- You don't have to inform third parties in terms of section 24(3) if this would involve a disproportionate effort on your part.

PART 6: PROCESSING OF SPECIAL PERSONAL INFORMATION

[51] Section 24(2).
[52] Section 24(3).

22. PROHIBITION ON PROCESSING OF SPECIAL PERSONAL INFORMATION

22.1. Special Personal Information is sensitive information, and the Processing thereof can constitute a significant or substantial intrusion of the Data Subjects' privacy. Such Processing is subject to stricter rules and is prohibited unless a **general or special exemption** applies.

22.2. Special Personal Information is defined as follows in section 26:

22.2.1. 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

22.2.2. the criminal behaviour of a Data Subject to the extent that such information relates to:

22.2.2.1. the alleged commission by a Data Subject of any offence; or

22.2.2.2. any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings.

Guidance notes

- Regard should be had to the Regulator's Guidance Note on Processing Special Personal Information ("**SPI Guidance Note**").
- In order to lawfully Process Special Personal Information, you should identify both a lawful basis under the general conditions for Processing and an authorisation for Processing under section 27. These do not have to be linked.

22.3. In terms of section 27(2) of POPIA, the Regulator may by notice in the Gazette authorise you to Process Special Personal information if the Regulator is satisfied that such Processing is:

22.3.1. in the public interest; and

22.3.2. appropriate safeguards have been put in place to protect the Special Personal information of the Data Subject.

Guidance notes

- Public interest is a wide and diverse concept that cannot, and should not, be limited in its scope and application. The definition of what constitutes public interest varies across jurisdictions and should be assessed on a case-by-case basis. In its very basic formulation public interest is the notion that an action or process or outcome widely and generally benefits the public at large (as opposed to a few or a single entity or person) and should be accepted or pursued in the spirit of

equality and justice.[53]

- Applications for authorisation to Process Special Personal Information must be made in the form included in the SPI Guidance Note.

23. GENERAL EXEMPTIONS

23.1. The general exemptions allow for the Processing of Special Personal Information:[54]

23.1.1. With the Consent of the Data Subject.[55]

Examples

- Consent would, for example, be required for the Processing of:
  - religious information in connection with products where religion is relevant;
  - health-related information other than for underwriting or assessment purposes.

23.1.2. If it is necessary to establish, exercise or defend a right or obligation in law.[56]

Examples

- You may have to disclose information about Data Subjects in legal proceedings in order to be able to defend your own position, e.g. when there is a dispute regarding the non-disclosure of medical information in a policy application form.
- You rely on the legal obligation imposed by FICA to Process Personal Information in order submit a suspicious activity report to the FIC when you know or suspect that a person is engaged in, or attempting, money laundering.
- You may have to disclose information about Data Subjects in line with a court order or arbitration proceedings.
- Insurers share medical and criminal data with other insurers (via Astute) to prevent fraud.

23.1.3. If the Processing is necessary to comply with an obligation of international public law.

[53] SPI Guidance Note, par 4.2.
[54] Section 27.
[55] Section 27(1)(a).
[56] Section 27(1)(b).

23.1.4. If the Processing is for historical, statistical or academic or scientific research purposes to the extent that:

23.1.4.1. the purpose serves a public interest and the Processing is necessary for that purpose; or

23.1.4.2. 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.[57]

23.1.5. If the information has deliberately been made public by the Data Subject.[58]

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

24. SPECIAL EXEMPTIONS

Race[59]

24.1. Personal information about Data Subjects' race may only be Processed when it is carried out to:

24.1.1. identify Data Subjects, but only where this is essential for that purpose; and

24.1.2. comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

Example

- You Process Personal Information relating to the Data Subject's race for B-BBEE / employment equity reporting purposes.

Trade union membership[60]

24.2. 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

[57] Section 27(1)(d).
[58] Section 27(1)(e).
[59] Section 29.
[60] Section 30.

- You should check that the trade union has the members' Consent to disclose their information.

Health or sex life[61]

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

Example

- Examples of a person's health or sex life include information relating to pregnancy, sexual orientation, physical or mental health, well-being, disability, birth, medical history, or blood type.

24.4. 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:

24.4.1. Medical professionals, healthcare institutions or facilities or social services, if such Processing is necessary for the proper treatment and care of the Data Subject, or for the administration of the institution or professional practice concerned.[62]

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

24.4.2.1. 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;

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

24.4.2.3. the enforcement of any contractual rights and obligations.[63]

Example

- An insurer may Process a Data Subject's health or sex life information to underwrite an insurance policy.

24.4.3. Administrative bodies, pension funds, employers or institutions working for them if such Processing is necessary for:

[61] Section 32.
[62] Section 32(1)(a).
[63] Section 32(1)(b).

24.4.3.1. 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

24.4.3.2. the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.[64]

24.5. POPIA requires that your Processing of 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 you and the Data Subjects.[65]If you are permitted to Process information concerning a Data Subject's health or sex life and are not subject to an obligation of confidentiality by virtue of office, profession or legal provision, you must treat the information as confidential, unless you are required by law or in connection with your duties to communicate the information to other parties who are authorised to Process such information.[66]

24.6. 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.[67]

Guidance notes

- If you wish to Process Personal Information about a Data Subject's inherited characteristics for purposes of providing life insurance, you should carefully assess whether you are authorised in terms of the general exemptions to Process the information, e.g. by obtaining Consent from the Data Subject and all the family members involved.
- 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.

Criminal behaviour or biometric information[68]

24.7. The prohibition on Processing Personal Information concerning Data Subjects' criminal behaviour or biometric information does not apply if:

24.7.1. the Processing is carried out by bodies charged by law with applying criminal law; or

24.7.2. the information has been obtained in accordance with the law.

[64] Section 32(1)(f).
[65] Section 32(2).
[66] Section 32(3).
[67] Section 32(4).
[68] Section 33.

Guidance note

- In terms of POPIA, the criminal behaviour of a Data Subject only extends to the alleged commission by the Data Subject of any offence, or any proceedings in respect of any offence allegedly committed by the Data Subject of the disposal of such proceedings.[69]

Examples

- You are appointed by SARS to act as its agent to provide information on Data Subjects for purposes of tax evasion.
- You comply with FICA's money laundering obligations.

PART 7 - PERSONAL INFORMATION OF CHILDREN

25. PROCESSING OF PERSONAL INFORMATION OF CHILDREN

Prohibition on Processing Personal Information of Children

25.1. You may not Process Personal Information concerning a Child unless a general authorisation applies.[70]

25.2. 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, to take any action or decision in respect of any matter concerning him or herself.

General authorizations

25.3. The following general authorisations allow for the Processing of Personal Information of Children:[71]

25.3.1. Processing is carried out with the prior Consent of a Competent Person.[72]

25.3.2. Processing is necessary to establish, exercise or defend a right or obligation in law.[73]

Example

- Where legislation so requires, tracing Children who are entitled to benefits

[69] Section 26(1)(b).
[70] Section 34.
[71] Section 35.
[72] Section 35((1)(a).
[73] Section 35(1)(b).

in terms of a product.

25.3.3. Processing is necessary to comply with an obligation of international public law.[74]

25.3.4. Processing is for historical, statistical or research purposes to the extent that:

25.3.4.1. the purpose serves a public interest and the Processing is necessary for that purpose; or

25.3.4.2. it would involve a disproportionate effort to ask for Consent,

and sufficient guarantees are provided to protect the privacy of the Data Subjects.[75]

25.3.5. If the information has been deliberately made public by the Child with the Consent of a Competent Person.

25.4. Upon your application and by notice in the Gazette, the Regulator may authorise you to Process the Personal Information of Children if the Processing is in the public interest and appropriate safeguards have been put in place to protect the Personal Information.

PART 8 - PRIOR AUTHORISATION

26. PROCESSING SUBJECT TO PRIOR AUTHORISATION[76]

26.1. You must obtain prior authorisation from the Regulator if you plan 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.[77]

Guidance notes

- Section 1 of POPIA and the Guidance Note on Application for Prior Authorisation ("**Prior Authorisation Guidance**") respectively define "*unique identifier*" as any identifier that is assigned to a Data Subject and is used by a Responsible Party for the purposes of the operations of that Responsible

[74] Section 35(1)(c).
[75] Section 35(1)(d).
[76] See definition of "*unique identifier*" for purposes of sections 57, 105 and 106 in Chapter 1.
[77] Section 57(1)(a).

Party and that uniquely identifies that Data Subject in relation to that Responsible Party.

- If you intend to link your unique identifiers with information Processed by other Responsible Parties for a purpose other than the one for which the identifier was obtained at collection, you will need to obtain prior authorisation.

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.
- You share information linked to a unique identifier with other companies in your group so that the information can be matched and the customer can be profiled for targeted campaigns.
- A credit provider collects an identity number to provide credit and links it with information from a credit bureau for the purpose of conducting a credit check and an affordability assessment.

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

Guidance notes

- The Prior Authorisation Guidance defines "*criminal behaviour*" as referring to, for example, a criminal record enquiry.
- The Prior Authorisation Guidance defines "*unlawful or objectionable conduct*" as including, but not limited to, any reference check pertaining to past conduct or disciplinary action taken against a Data Subject.
- The Prior Authorisation Guidance provides that this section may be applicable to any person contracted to conduct a criminal record enquiry, reference check pertaining to the past conduct or disciplinary action taken against a Data Subject. Note that the requirement for prior authorisation has a wider application than the definition of "*criminal behaviour*" under section 26 (Special Personal Information).

26.1.3. Process information for the purposes of credit reporting.

Guidance note

- Credit reporting as defined [78] would not apply to Responsible Parties

[78] "*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*."

supplying information to third parties (such as credit bureaux) to enable such third parties to in turn compile credit reports.

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.

Guidance notes

- If you intend to transfer, for any purposes (such as storage or subsequent updating or modification) Special Personal Information or Personal Information of Children to a third party outside the boarder of the Republic of South Africa, you should assess whether the third party in the foreign country is subject to law, binding corporate rules, or binding agreement which provides an adequate level of protection that effectively upholds principles for reasonable Processing of the information that are substantially similar to the 8 conditions for the lawful Processing of Personal Information set out in POPIA. If these countries do not meet the above criteria, you will have to obtain prior authorisation.
- When dealing with the cross-border transfer of Personal Information in respect of juristic persons, it should be borne in mind that very few other countries provide for the protection of Personal Information in respect of juristic persons and that this may impact the consideration of adequacy,
- In addition to the requirement for prior authorisation, the provisions of section 72 (transborder flows of information) apply.

26.2. You only have to obtain the prior authorisation from the Regulator 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.

PART 9 - UNSOLICITED ELECTRONIC COMMUNICATION, COOKIES AND AUTOMATED DECISION MAKING

27. ELECTRONIC DIRECT MARKETING

27.1. The Processing of Personal Information of Data Subjects for the purpose of Electronic Direct Marketing, including automatic calling machines[79], facsimile machines, SMSs or e-mail is prohibited, unless the Data Subject:

27.1.1. has given their Consent to the Processing;[80][81]

[79] "*Automatic calling machine*" means a machine that is able to do automated calls without human intervention.
[80] Section 69(1)(a).
[81] Consent must be in the form of Form 4 to the POPIA Regulations.

27.1.2. is a customer of yours and if:[82]

27.1.2.1. the Data Subjects' contact details were obtained in the context of the sale of your products or services;

27.1.2.2. the Personal Information of the Data Subjects is Processed for the purpose of the Direct Marketing of your own similar products or services; and

27.1.2.3. the Data Subject has 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 if the Data Subject has not initially refused such use ("**Soft Opt-in**").

27.2. You may approach Data Subjects only once in order to obtain Consent for this type of Processing.[83] Such Consent must be obtained in the prescribed manner and form.[84]

27.3. Any communication for the purpose of Electronic Direct Marketing must contain:[85]

27.3.1. details of the identity of the sender or the person on whose behalf the communication has been sent; and

27.3.2. an address or other contact details to which the recipient may send a request that such communications cease.

Guidance notes

- Data Subjects may object, at any time, to the Processing of Personal Information for purposes of Electronic Direct Marketing.
- The definition of Electronic Direct Marketing doesn't cover electronic mail sent for administrative or customer service purposes, for example, emails to advise changes to terms and conditions or advise someone of a problem with their account. These types of messages are often referred to as "service messages". They don't count as Electronic Direct Marketing if you use them purely for administrative purposes. This is because you aren't advertising or marketing to customers. However, if you include promotional content within your service message, then the message counts as Electronic Direct Marketing, for example, content with the aim of getting your customer to buy more products.
- When marketing is conducted by means of unsolicited Electronic Communications, additional rules apply. This means you should not rely on grounds other than Consent (by means of Form 4) and Soft Opt-ins, whilst you may, for other types of

[82] Section 69(1)(b).
[83] Section 69(2)(a).
[84] Section 69(2)(b) and Form 4.
[85] Section 69(4).

Direct Marketing, be able to rely on the legitimate interest ground – see **Guidance Notes** on legitimate interests of the Responsible Party above.

- You should only use the Soft Opt-in if all of the following conditions apply:
  - you want to send marketing by electronic means to existing customers, provided they have not previously opted out;
  - you collected their contact details directly from them;
  - you collected their details during a sale, or negotiations for a sale, of your products or services;
  - you want to use their details to send them marketing about your similar products and services;
  - you give them a clear, simple way to opt-out, or to say no to your marketing, when you collect their details;
  - you give them a clear, simple way to opt-out, or change their mind about your marketing, in each message you send.
- A person doesn't actually need to buy anything from you to trigger the Soft Opt-in. It is enough if "negotiations for a sale" took place. This means that they should have actively express an interest in buying your products or services, for example by requesting a quote or asking for more details of what you offer. You should have some form of express communication.
- The Soft Opt-in specifically uses the word "*sale*" and refers to "*products and services*". This means it doesn't apply to details collected where there is no sale (or such a negotiation), or where there is no product or service involved, e.g. campaigning.
- You can only send electronic mail about your similar products or services. The key question is whether people reasonably expect Electronic Direct Marketing about your particular product or service. This is likely to depend on the context, including the type of business you are and the category of product.
- You should make it simple for customers to change their mind and opt-out or unsubscribe. Opportunities for opt-outs, include, but are not limited to, replying directly to the message, or clicking a clear 'unsubscribe' link, referring them to your website to unsubscribe or offering a stop message to a short code number.
- The Soft Opt-in doesn't apply to bought-in marketing lists. This is because as part of the Soft Opt-in you must collect the details directly from the person you want to send marketing to during the course or negotiation of a sale of a product or service. Clearly this doesn't apply to details you got from a third party. There is no such thing as a third-party marketing list that is Soft Opt-in compliant. You may, however, rely on the Consent basis if you ensure that the customer has Consented to their information being distributed to you for Direct Marketing purposes.
- You should add the contact details of people who withdraw their Consent or unsubscribe to your 'do not contact' or suppression list. Using such a list helps you to comply, as you can check against it and avoid sending Electronic Direct Marketing to anyone who has told you not to. It is good practice to also compare your list to that of the DMASA.

Examples

- A customer completes an online enquiry form asking for more details about a product. This is enough to meet this part of the Soft Opt-in.
- A customer logs into your website to browse its range of products. This would not be enough to constitute negotiations and this part of the Soft Opt-in.

28. COOKIES

Guidance notes

- Although POPIA does not specifically mention cookies, it does apply to cookies:
  - The definition of "*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*" (which can include cookies);
  - The definition of "*personal information*" includes an online identifier (which can include cookie identifiers);
  - The definition of a "*unique identifier*" in terms of POPIA is "*any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party*" (which can include cookie identifiers).
- The Regulator may pass regulations to specifically regulate the use of cookies in South Africa, but has not indicated that this will happen. The Regulator will probably follow international guidelines on cookies, e.g. that a user merely scrolling on a website does not amount to informed Consent.
- As long as cookies are not used "*for a purpose other than the one for which the identifier was specifically intended at collection*", you should not need to get prior authorisation from the Regulator to use cookies.
- If you use cookies for the purpose of Direct Marketing and the Data Subject is not a customer of yours, you should get the Data Subject's Consent. It will be very hard for any website owner to know who a visitor to its website is and this practically means that POPIA would require a cookie notice/banner asking consent to use cookies to profile the user and subsequently use the Personal Information for marketing, analytics and online behavioural advertising, and a cookie policy, which should be distinguished from your Privacy Notice - they are two different subjects that should be dealt with separately. Your cookie notice should also provide a link to your cookie policy.
- Even if the purpose is not Direct Marketing, a cookie collects Personal Information and therefore you should take reasonably practicable steps to ensure the Data Subject is aware of the collection and the other aspects requiring notification in terms of section 18.

Examples

- If you utilise cookies on a website to obtain Personal Information from Data Subjects with a view to using that information for Processing like tracking and profiling for purposes of on selling and/or further marketing to the Data Subjects, Consent will have to be obtained due to the nature of the Processing operations.
- A cookie is necessary if your website cannot serve a user without it. Note, however, that it is what's necessary for the *user*. Cookies for analytics and advertising preferences are *not* considered necessary from a legal perspective, because your website can serve a user without tracking them for either website usage analysis or advertising purposes.
- Examples of cookie uses that require Consent include:
  - social media plug-ins;
  - social media tracking;
  - on-line advertising;
  - analytics - You are likely to view analytics as 'strictly necessary' because of the information they provide about how visitors engage with your service. However, you cannot use the strictly necessary exemption for these. Consent is required because analytics cookies are not strictly necessary to provide the service that the user requests. For example, the user can access your online service whether analytics cookies are enabled or not.
- Examples of cookies where Consent is not likely to be required (subject to the purpose limitation):
  - user input;
  - authentication;
  - security
  - user preference;
  - network management.

29. DECISIONS BASED ON THE AUTOMATED PROCESSING OF PERSONAL INFORMATION

29.1. 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:[86]

[86] Section 71(1).

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

29.1.1.1. the request of the Data Subjects in terms of the contract has been met; and

29.1.1.2. appropriate measures have been taken to protect the Data Subjects' legitimate interests; or

29.1.2. is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of the Data Subjects.

29.2. 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

- Automated individual decision-making is a decision made by automated means without any human involvement. These rights can be seen as safeguards against the risk that a potentially damaging decision is taken without human intervention.
- POPIA does not prevent the use of analytics in decision-making or research as such, but it does provide for certain duties and restrictions, which could amongst other relate to the de-identification of Personal Information. Practically this might require that certain information will be redacted or in fact removed in totality, or it may require that a separate database will be created for purposes of testing new systems or for purposes of analysis.
- You should provide the Data Subject with the opportunity to make representations about the decision and to provide the 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 such representation.
- A legal effect is something that affects someone's legal rights. Similarly significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application.
- You should only conduct automated decision making on the basis stipulated in section 71(2), such as the conclusion or performance of a contract (if the request of the Data Subject has been fulfilled and the Data Subject's legitimate interests are protected). No other grounds for Processing may be relied on.

PART 10 – CROSS BORDER TRANSFERS

30. TRANSFERS OF PERSONAL INFORMATION OUTSIDE SOUTH AFRICA

30.1. You may not transfer Personal Information about Data Subjects to a third party in a foreign country unless:

30.1.1. the third party in question is subject to a law, binding corporate rules[87] or binding agreement which provides an adequate level of protection that:[88]

30.1.1.1. 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

30.1.1.2. 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;

30.1.2. the Data Subject has given their Consent; or

30.1.3. the transfer is necessary for the performance of the contract between the Data Subject and yourself, or for the implementation of pre-contractual measures taken in response to the Data Subject's request; or

30.1.4. transfer is necessary for the conclusion or performance of a contract concluded between yourself and a third party in the Data Subject's interest; or

30.1.5. transfer is for the benefit of the Data Subjects, and:

30.1.5.1. it is not reasonably practicable to obtain the Consent of the Data Subjects to that transfer; and

30.1.5.2. if it were reasonably practicable to obtain such Consent, the Data Subjects would be likely to give it.

Guidance notes

- You should check if your IT contract service providers, such as SAAS providers, who Process (e.g. store) Personal Information on your behalf in another country are subject to a law, binding corporate rules or binding agreement which provides an adequate level of protection that upholds principles for reasonable Processing of the information substantially similar to POPIA, including the transfer of Personal Information to a third party in a foreign country or whether the transfer is necessary for the performance of a contract with the Data Subject. If not, you will have to obtain the Consent of the Data Subject, unless it is not reasonably practicable and the Data Subject would be likely to give it. Please note the **Guidance Notes** relating

[87] "*Binding corporate rules*" means 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. "*Group of undertakings*" means a controlling undertaking and its controlled undertakings.
[88] Section 72(1).

to juristic persons under paragraph 26.1.4 above.

- In addition to the requirement for an Operator agreement, you will have to comply with the conditions for Processing set out in section 72.
- IT services contracts are often offered on the IT provider's standard terms and conditions. In the EU and UK, they are likely to contain a Data Processing Addendum to the Agreement, even if the IT service provider is an Operator ("data processor"). You should not automatically assume that this is sufficient for POPIA purposes and should check such Addendums to make sure they cover what you would want to be covered in an Operator Agreement.
- If your Operator sub-contracts to service providers located outside of South Africa, the Processing is still subject to section 72.

PART 11 – COMPLAINTS AND OFFENCES

31. COMPLAINTS

31.1. Any person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with the protection of the Personal Information of a Data Subject.[89]

31.2. You or the Data Subject may, in terms of section 63(3), submit a complaint to the Regulator in the prescribed manner and form if aggrieved by the determination of an adjudicator.[90]

32. UNLAWFUL ACTS BY RESPONSIBLE PARTIES IN CONNECTION WITH ACCOUNT NUMBERS

32.1. An "*account number*" is defined in section 105(5) to mean 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.

32.2. If you contravene any of the information protection conditions insofar as they relate to the Processing of an account number, you are guilty of an offence if:[91]

32.2.1. the contravention is of a serious or persistent nature and is likely to cause substantial damage or distress to the Data Subjects; and

[89] Section 74(1).
[90] Section 74(2).
[91] Section 105.

32.2.2. you 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.

32.3. It is a valid defence to such a charge to contend that you have taken all reasonable steps to comply with the information protection conditions.

HISTORY OF DOCUMENT

Date	Published / Amended
July 2021	First published.
March 2024	Competition law review and developments update.

RESPONSIBLE COMMITTEE & SENIOR POLICY ADVISER

Responsible ASISA Board Committee	Regulatory Affairs Board Committee
Responsible Working Group	Protection of Personal Information Act Working Group
Responsible Senior Policy Advisor	ASISA Point Person to the Protection of Personal Information Act Working Group