British
High Commission
Pretoria

Data Protection Toolkit Guidance

Responding to South Africa's Protection of Personal Information (POPI) Act of 2013

For Small, Medium and Micro Enterprises (SMMEs)

Data Protection Toolkit Guidance Pack

The data protection toolkit guidance pack consists of information and templates that can be adapted and used by SMMEs. The pack consists of the following:

SECTION 01

Summary of Data Protection Toolkit

Summary

FOREWORD

Data plays a key role in the activities of an SMME. The Protection of Personal Information (POPI) Act came into effect on 1 July 2021 and provides both challenges and opportunities for SMMEs. This toolkit aims to support SMMEs to better implement the elements of data protection associated with the POPI Act. Aligning and complying with the new law is a challenge for all organizations, big or small. It does, however, provide an opportunity to refresh policies and procedures related to the safe stewardship of data. This legislation is generating momentum and enterprises are identifying risks and developing coherent plans to mitigate these. The POPI Act also places a firm emphasis on citizens being informed on the use of data and their associated rights. SMMEs are entrusted to process personal information so it is imperative that they are complying with the 8 Principles of the POPI Act.

PURPOSE

This toolkit is aimed at SMMEs in South Africa that want to achieve data security and data protection. It provides steps that can help SMMEs develop the minimum required processes and documentation in order to be compliant with the legislation. However, SMMEs should follow all guidance as set out by the Information Regulator.

Summary

INTENDED OUTCOMES	1. Demystify the language associated with data protection, and the POPI Act. 2. SMMEs are aware that responsibility for compliance with data protection legislation lies with them. 3. SMMEs will understand how to effectively monitor and review compliance, working closely with the appointed Information Officer and Deputy Information Officer. 4. Become familiar with the conditions and lawful basis for processing that are most relevant to business activity. 5. Increase the basic cyber hygiene and controls amongst SMME owners.
IMPORTANT NOTE	It is important to note that this document provides tips and guidance only. It does not constitute formal legal guidance and the SMME is ultimately responsible for its own data protection procedures and compliance with the POPI Act. The information processed by SMMEs remains their responsibility.

SECTION 02

Summary of the POPI Act

Summary of the POPI Act

Section 14 of the Constitution of the Republic of South Africa, 1996 (the "Constitution") provides everyone with the right to privacy. POPIA was enacted in order to give effect to section 14 of the Constitution, to promote the protection of information which is of a personal nature and which is processed by both public and private entities.

The main objective of the POPI Act is the promotion of the protection of information, which is of a personal nature and which is processed by both public and private bodies.

The POPI Act introduces conditions which need to be satisfied as minimum requirements in the context of processing of personal information. However, the POPI Act recognises that a balance needs to be struck as many companies need to process personal information in the day-to-day running of their businesses. Accordingly the POPI Act does not prohibit the processing of Personal Information but rather prohibits the unlawful processing of Personal Information.

The POPI Act enables data subjects, to bring civil actions against firms for data breaches. Violations of the Act could result in fines or compensation for damages. Administrative fines may be as high as R10million. The impact of a fine on SMMEs could be detrimental (especially given the number of SMMEs already impacted by the pandemic), and poor cyber awareness and hygiene will result in the increased likelihood of a successful attack by cyber threat actors.

The POPI Act introduces 8 Principles:

Principle 1: Accountability

Principle 2: Processing Limitation

Principle 3: Purpose Specification

Principle 4: Further Processing Limitation

Principle 5: Information Quality

Principle 6: Openness

Principle 7: Security Safeguards

Principle 8: Data Subject Participation

What does the POPI Act mean for SMMEs

As of 30 June 2021, all organisations are required to adhere to the POPI Act to ensure that all processing of personal information complies with the requirements of the Act. This includes compliance with the prescribed conditions for the lawful processing of personal information.

The conditions for the lawful processing of personal information by or for a responsible party are driven by the 8 Principles of the POPI Act .

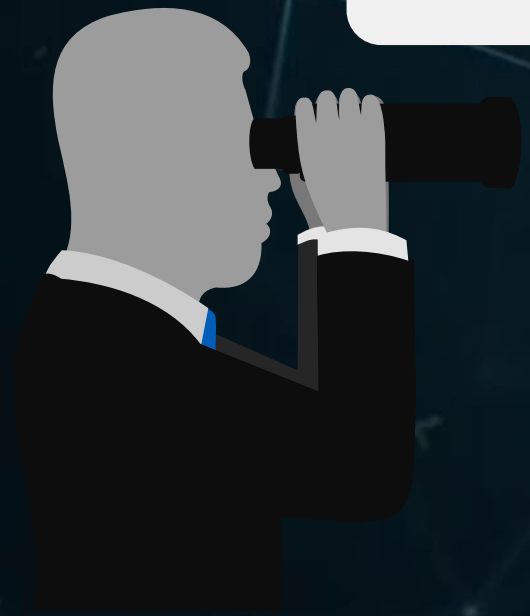
The POPI Act not only applies to private and public entities in South Africa, but is also applicable to entities outside of South Africa that make use of automated or non-automated means for processing personal information in South Africa, unless such means are solely used to forward personal information through South Africa.

The POPI Act compliance necessitates a thorough understanding of an organisation's data, collection of data, the risk that a breach of data and the existing controls in place to mitigate against those risks (whether internal or external to the organisation). An assessment of how the organisation processes personal information with reference to the requirements for the lawful processing of such personal information, as set out in the POPI Act, will be required as an initial first step in any POPI Act compliance programme.

Consequences of failing to comply to the POPI Act

Contravention of certain provisions of the Act will be deemed to be an offence in terms of POPIA. Persons having convicted of an offence under POPIA will be liable to a fine of up to R10 million for administrative fees or imprisonment for a period of up to 10 years or to both a fine and imprisonment.

Organisations may be exposed to the financial cost of information security breach discovery and ensuring that the Information Regulator and each relevant data subject is notified of the information security breach.



Organisations may be exposed to civil damages, which may be instituted by the data subject (or Information Regulator on behalf of the data subject) in a civil court for a breach of the lawful processing provisions prescribed by POPIA, non-compliance of certain listed sections of POPIA, or breach of the provisions of a code of conduct issued in terms of POPIA

Key Definitions of the POPI Act (1/2)

The POPI Act only applies in respect of information relating to an identifiable, living, natural person. There is also an important sub-category of Personal Information known as Special Personal Information as seen in the block on the right. The POPI Act generally prohibits the processing of Special Personal Information unless an specific exception applies.

In terms of POPIA, personal information is defined as:

Information relating to the education, medical, blood type, biometrics, financial, criminal, or employment history of a person.

Information regarding the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical/mental health, well-being, disability, religion, conscience, belief, culture, language and birth of a person.

Any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person.

The name of the person if it appears with other personal information relating to the person of if the disclosure of the name itself would reveal information about the person.

The personal opinions, views or preferences of a person; or about the person by another individual.

Correspondence sent by the person that is implicitly or explicitly private or confidential in nature or further correspondence that would reveal the contents of the original correspondence.

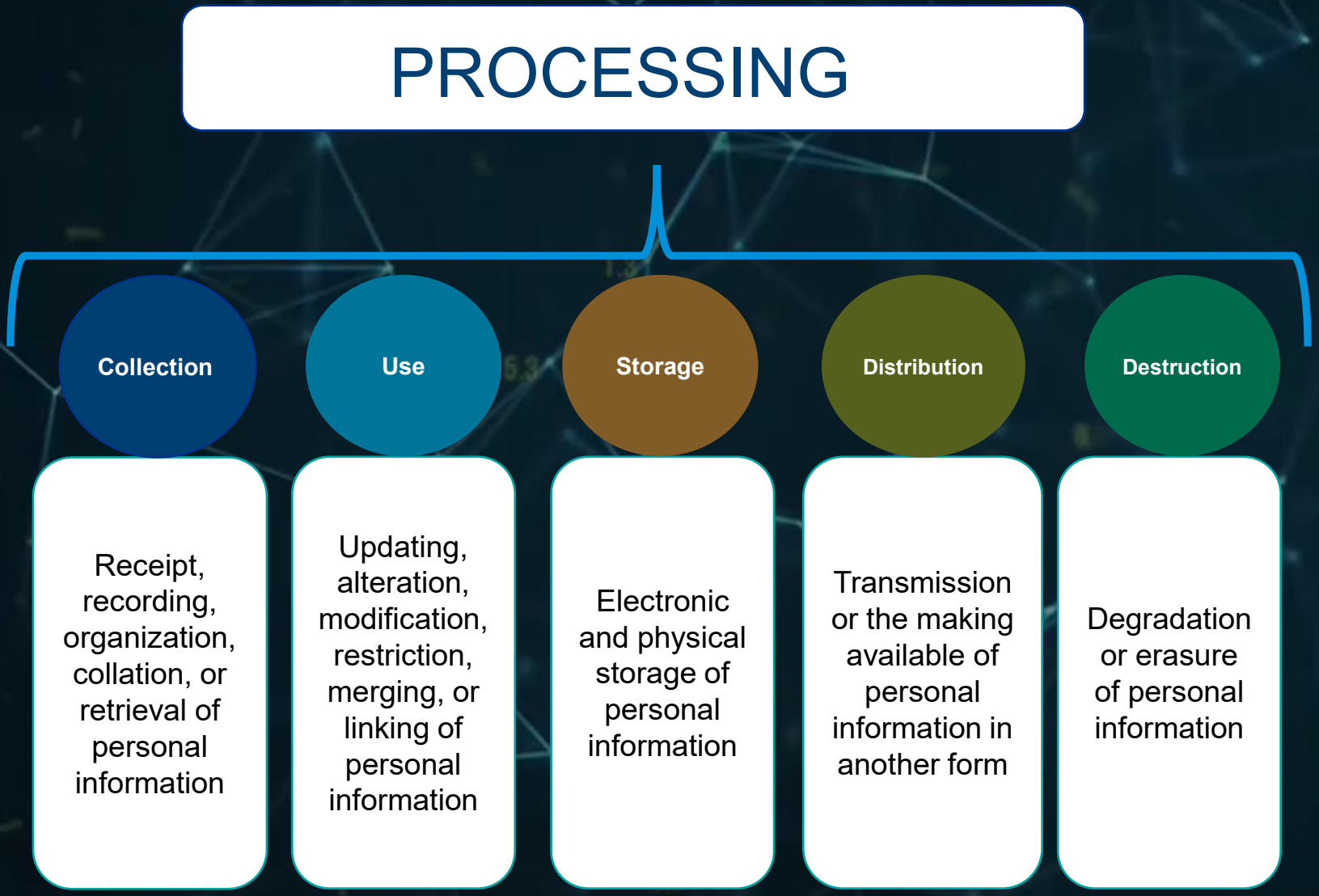
Special Personal Information

- Religious/philosophical beliefs
- Race/ethnic origin
- Trade union membership
- Political persuasion
- Health/sex life
- Biometric information
- Criminal behaviour of data subject (alleged commission / proceedings / disposal of proceedings)

General prohibition on processing of special personal information

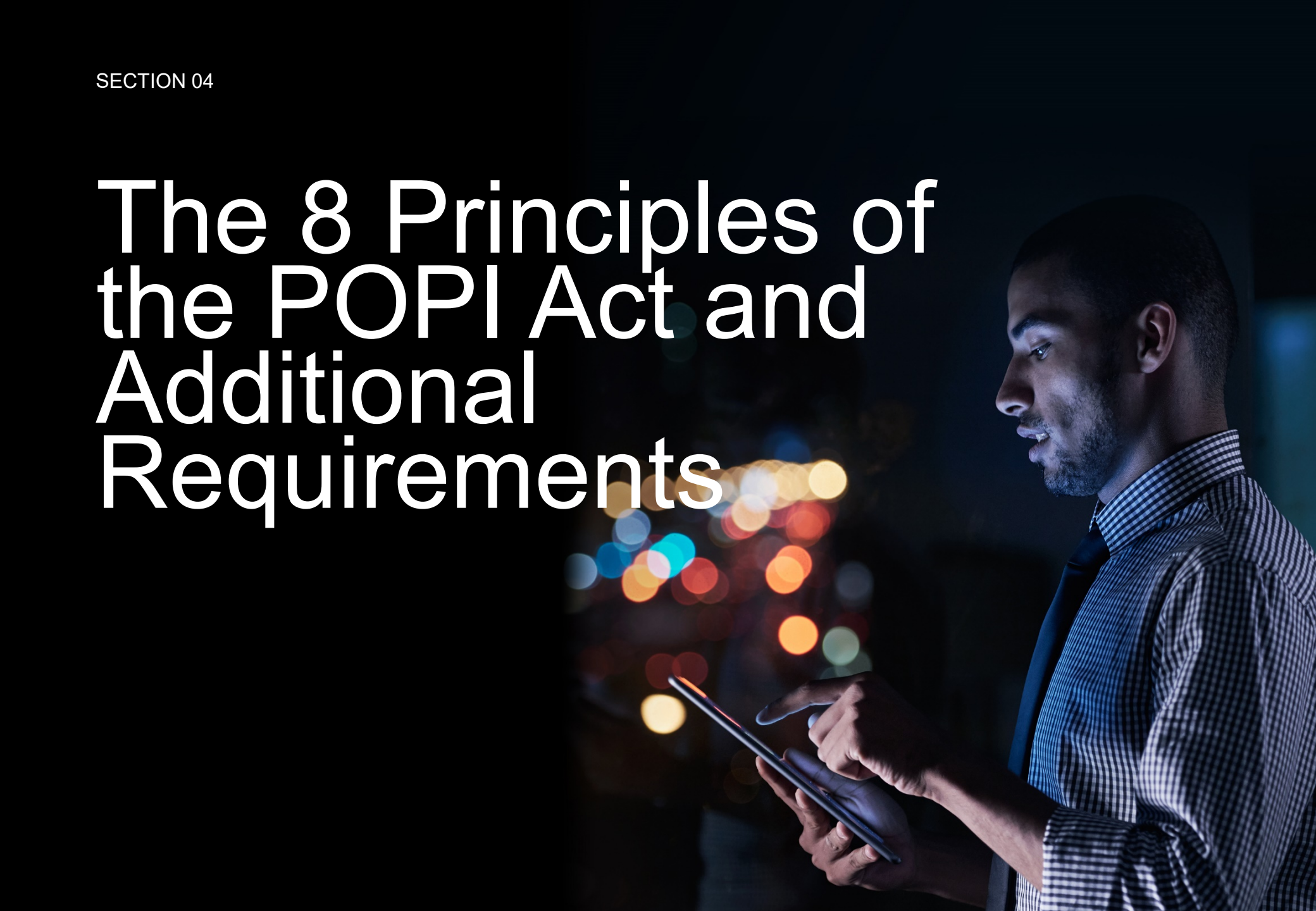
Key Definitions of the POPI Act (2/2)

Another key definition is "PROCESSING" which effectively describes the manner in which Personal Information can be used and includes Collection and Destruction and everything in between.



SECTION 04

The 8 Principles of the POPI Act and Additional Requirements



Principle 1: Accountability

1. DEFINITION

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

2. CONTEXT

The organization must ensure that the 8 processing conditions of the POPI Act and measures which give effect to the conditions are complied with.

3. CONTROLS

1. Appointing an Information Officer and Deputy Information Officer (depending on the size of the organization) who will be tasked with the responsibility of compliance in your organization.
2. This individual will drive compliance with the POPI Act.
3. Performing training and awareness amongst staff members regarding their roles and responsibilities when dealing with personal information.
4. Develop guidelines and awareness materials which support employees in applying POPI Act Principles.

4. MINIMUM REQUIREMENTS

1. Determine whether the POPI Act applies to your organisation.
2. Appoint and register Information Officers and, where appropriate, Deputy Information Officers. Make sure their roles and responsibilities are clearly communicated.
3. Perform training and awareness
4. Develop policies, procedures and/or guidelines must be in place.

Principle 2: Processing Limitation

1. DEFINITION

Personal Information may only be processed lawfully and in a reasonable manner that doesn't infringe rights of a data subject. Only the minimum Personal Information necessary to achieve the purpose of collection should be processed. Further there must be a lawful basis or justification to process Personal Information as set out in Section 11 of the POPI Act. Finally, Personal Information should be collected directly from the data subject rather than an indirect source unless an exception specified in Section 12 of the POPI Act applies.

2. CONTEXT

(i) Processing Personal Information must be for a lawful and reasonable;
(ii) Personal Information processed must be adequate, relevant and not excessive
(iii) Processing may only occur whether there is a lawful justification (which may include consent) and,
(iv) Collection of Personal Information should be directly from the data subject unless an exception applies.

3. CONTROLS

1. Consider the nature of your processing activities and whether they are unreasonably infringing the data subject's right to privacy
2. Document and review the personal information collected and whether it is all necessary to achieve the purpose for collection.
3. Consider and document the lawful basis for processing different types of Personal Information. If consent is one of those bases then ensure you have obtained written consent.
4. Collect Personal Information directly from the Data Subject unless you are sure an exception in section 12 of the POPI Act applies.

4. MINIMUM REQUIREMENTS

1. Where consent is relied on it is recommended that this is obtained in writing for evidentiary purposes and that template consent forms are drafted for this purpose.
2. Review your forms and modes of collecting personal information to ensure that the minimum information is being collected. Also consider you processing activities and delete personal information which is not relevant or which is excessive.
3. It is recommended that you maintain a record of your processing activities and the lawful basis for collecting different sets of Personal Information for example in a Personal Information Inventory.

Principle 3: Purpose Specific

1. DEFINITION

Personal Information may only be collected for specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. Records of Personal Information must not be maintained any longer than is necessary to achieve that lawful purpose unless an exception in section 14 of the POPI Act applies.

2. CONTEXT

1. There must be a lawful purpose for collecting personal information
2. Personal information must be destroyed, deleted or deidentified once the purpose for collection has been achieved unless an exception in section 14 of the POPI Act applies (for example the law requires the Responsible Party to retain the record).

3. CONTROLS

1. Personal Information should only be gathered for specific, explicit and lawful purposes. The purpose for personal information should be documented and adhered to.
2. Personal Information records must be destroyed, deleted or deidentified once the purpose for collection has been achieved unless an exception applies allowing or requiring the records are retained for a longer period.
3. The organization should be able to keep track of the personal information records it holds and the date that each needs to be destroyed.
4. Policies and procedures to be followed to destroy personal information should be formalized.

4. MINIMUM REQUIREMENTS

1. Information Asset Register
2. Retention Policy and Schedule (Retention Schedule included in the Information Asset Register)
3. Record of destruction

Principle 4: Further Processing Limitation

1. DEFINITION

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

2. CONTEXT

Personal Information may not be processed for a secondary purpose unless that processing is compatible or in accordance with the original purpose.

3. CONTROLS

1. Training and awareness should be conducted to ensure employees understand that they should not perform secondary processing which is incompatible with the original purpose.
2. If further processing is incompatible with the original purpose then obtain consent of the data subject or record the exception that applies in terms of Section 15(3) of the POPI Act.

4. MINIMUM REQUIREMENTS

1. Perform training and awareness
2. Obtain signed consent forms in respect of further processing activities which are incompatible with the original purpose for which information is collected. Alternatively, record the other exception that applies and allows for further processing.

Principle 5: Information Quality

1. DEFINITION

The responsible party must take reasonable steps to ensure that the Personal Information collected is complete, accurate, not misleading and updated where necessary.

2. CONTEXT

The organization must ensure that Personal Information is complete, accurate, reliable and up-to-date.

3. CONTROLS

1. Collect Personal Information directly from the data subject or reliable sources
2. If you intend on using the Personal Information in the future, you should take proactive steps to ensure the Personal Information remains accurate (e.g. by reaching out to the data subject at regular intervals to request him/her to advise if his/her Personal Information has changed)
3. Data Subjects must be given details of how to update their information.

4. MINIMUM REQUIREMENTS

1. Review data collection processes
2. Remind data subjects to update their personal information if it has changed and advise them of the process to update their Personal Information.
3. Information Asset Register which is updated regularly.
4. Develop a process to update Personal Information records.
5. Consider if there may be duplication of records across the different systems which need to be reconciled.

Principle 6: Openness

1. DEFINITION

The Data Subject whose information you are collecting must be aware that you are collecting his/her/its Personal Information and the purpose for which the information will be used. You must be transparent with data subjects and provide them with a privacy notice / privacy statement which contains all the information prescribed by section 18 of the POPI Act. You must also maintain documentation of all processing activities.

2. CONTEXT

The Data Subject to be made aware that Personal Information is being collected by the organization and the minimum information prescribed by Section 18. The organization should maintain documentation for all its processing activities required in terms of the Promotion of Access to Information Act (PAIA).

3. CONTROLS

1. Develop a privacy notice / privacy statement which is published on your website or otherwise prominently displayed at your premises or can be provided to data subjects by other means.
2. If personal information is collected directly from the Data Subject, the data subject must be informed of the purpose and other prescribed information before collection. If personal information is being collected indirectly, then the data subject must be informed of this information as soon as reasonably practicable after the collection of Personal Information.
3. Where you use CCTV, ensure that notices are prominently displayed and explain the purpose for which footage will be used.
4. Develop or enhance the manual required in terms of the Promotion of Access to Information Act ("PAIA Manual") .

4. MINIMUM REQUIREMENTS

1. Perform training and awareness
2. Obtain signed consent forms in respect of further processing activities which are incompatible with the original purpose for which information is collected. Alternatively, record the other exception that applies and allows for further processing.

Principle 7: Security Safeguards

1. DEFINITION

A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—

(a) loss of, damage to or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information.

2. CONTEXT

Personal Information must be kept secure against the risks of loss, unauthorized access, interference, modification, destruction or disclosure.

3. CONTROLS

1. Determine the following:
(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
(b) establish and maintain appropriate safeguards against the risks identified;
(c) regularly verify that the safeguards are effectively implemented; and
(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
(e) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.
(f) Ensure operators enter into a written agreement that requires compliance with the above controls and requires the operator to notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

4. MINIMUM REQUIREMENTS

1. Draft data security policies and procedures
2. Draft Data Breach Notifications, policies and procedures
3. Draft incident management plan and playbooks.
4. Include controls into operator agreements

Principle 8: Data Subject Participation

1. DEFINITION

Data Subjects may request whether their Personal Information is held, as well as the access to those records. Data Subjects may also request the correction and/or deletion of the Personal Information held about them if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, obtained unlawfully or the organisation is no longer authorised to retain it.

2. CONTEXT

Data Subjects may request access to Personal Information held by the organisation about the data subject. In certain circumstances, data subjects may seek the correction or destruction of their Personal Information from the organisation's records.

3. CONTROLS

1. There should be processes in place to ensure that a request from a Data Subject is managed and complied with if legitimate.
2. Employees should receive training regarding the manner in which data subject participation rights will be handled by the organization. It should be clear what the process is to employees who may receive such requests.

4. MINIMUM REQUIREMENTS

1. Data Subject Access policies and procedures must be in place
2. Employees should receive training regarding the process to be followed in the case of a privacy complaint or where a data subject exercises his/her/its rights in terms of the POPI Act

Additional Requirements

The commencement of the POPI Act has changed the specific processing requirements that are listed below. However, these requirements are specific to the nature of the data subject, and the organization's business activities. SMMEs are encouraged to download and read guidance notes that are updated on a regular basis by the Information Regulator on their website: . Home I Information Regulator SA (justice.gov.za)

Additional Requirements for the POPI Act

- **DIRECT MARKETING**
- **PROCESSING OF SPECIAL INFORMATION**
- **PROCESSING OF CHILDREN'S PERSONAL INFORMATION**
- **PRIOR AUTHORIZATION**
- **AUTOMATED DECISION MAKEING**
- **INTERNATIONAL TRANSFERS**
- **COMPLAINTS AND INVESTIGATION MANAGEMENT**

SECTION 03

Guidance for Templates

Mapping of Templates to Principles

	Templates	
POPI Act 8 Principles	**From the Information Regulator's Website**	**Within this toolkit**
Accountability	https://www.justice.gov.za/inforeg/docs/forms/InfoRegSA-eForm-InformationOfficersRegistration-2021.pdf https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf	Policies, Processes and Procedures Duties and Responsibilities Manual developed by Information Regulator
Processing Limitation	https://www.justice.gov.za/inforeg/docs/forms/PAIA-Manual-Template-Private-Body.docx Also, refer to the Information Regulator's website for updated guidance notes and templates that can be used to satisfy the POPI Act's Principles.	Privacy Notice and Consent Template Data Privacy Policy Template
Purpose Specific		Information Asset Register Retention Policy and Schedule (Retention Schedule included in the Information Asset Register) Record of destruction
Further Processing Limitation		Proof of Consent Template
Information Quality		Information Asset Risk Register Template
Openness		Breach Notification Letter Template Incident Management Playbooks
Security Safeguards		Risk Register Template
Data Subject Participation		Data Subject Access Policies and Procedures

*Disclaimer: This section is for reference purposes only. It does not constitute as legal advice, and is not intended to be a substitute for legal advice. SMMEs should seek legal advice or other professional advice in relation to templates

Privacy Notice and Consent Template

GUIDANCE TO READ BEFORE USING DOCUMENT

- *Purpose* — *This template can be used by the organisation to assist in the creation of a Privacy Notice which can be administered to Data subjects and also used to request their consent.*
- *Responsibility* — *The organisation*
- *Usage* — *Administered by the Information Officer and Deputy Information Officer to Data Subjects*

Follow this link to access the template: South Africa GCA Cybersecurity Toolkit - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

Acceptable Use Policy Template

GUIDANCE TO READ BEFORE USING DOCUMENT

- *Purpose* — *This policy, developed by the SANS Institute (free to use), describes the practices and constraints that a user must agree to in order to gain access to a corporate network or use company-owned devices.*
- *Responsibility* — *The organisation*
- *Usage* — *By all users within the organisation, including third party vendors*

Follow this link to access the template: South Africa GCA Cybersecurity Toolkit - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

Data Privacy Policy Template

GUIDANCE TO READ BEFORE USING DOCUMENT

•*Purpose*	*This policy should be used by the business to outline the scope of the information that will be collected where and how the information will be collected, and how the business will ensure that the information is kept confidential and secure*
•*Responsibility*	*The organisation*
Usage	*This policy should be provided to data subjects before collecting their personal information directly from them or as soon as possible after collection from another source.*

Follow this link to access the template: South Africa GCA Cybersecurity Toolkit - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

Breach Notification Letter Template

GUIDANCE TO READ BEFORE USING DOCUMENT

•*Purpose*	*This letter should be completed in the event that there is a breach of access to a part or a whole of personal information collected, used and/or stored by the business. The letter should contain detail the breach, how it impacts the owner(s) of the data and the investigation process that Company X is following to prevent harm to the respective owners and to prevent any further breaches.*
•*Responsibility*	*The organisation*
•*Usage*	*To be completed by the Information Officer with input from the Head of Information Security*

Follow this link to access the template: South Africa GCA Cybersecurity Toolkit - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

Information Asset Register Template

GUIDANCE TO READ BEFORE USING DOCUMENT

- *Purpose* — *This is a repository of the company's Information Assets; either physical or virtual. It is important that this register is kept up-to-date and contains accurate information.*
- *Responsibility* — *The organisation*
- *Usage* — *Should be used internally*

Follow this link to access the template: South Africa GCA Cybersecurity Toolkit - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

Data Collection Policy Template

GUIDANCE TO READ BEFORE USING DOCUMENT

- *Purpose* — *This policy should be used by the business as a guide when collecting personal information from different people and/or businesses and should contain details of the type of data collected, the specific purpose of collecting the data and how the data will be stored and disposed.*
- *Responsibility* — *The organisation*
- *Usage* — *Information Officer should be the policy owner and ensure that the policy is shared and adhered to by all employees, subsidiaries and third parties*

Follow this link to access the template: South Africa GCA Cybersecurity Toolkit - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

Retention Policy Template

GUIDANCE TO READ BEFORE USING DOCUMENT

- *Purpose* — *This policy should be used to ensure that records on Personal Information is properly retained and destroyed in accordance with legal, regulatory and company requirements.*
- *Responsibility* — *The organisation*
- *Usage* — *The Information Officer and the Deputy Information Officer are the owners of this policy. The retention schedule can be found within the Information Asset Register.*

Follow this link to access the template: South Africa GCA Cybersecurity Toolkit - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

Record of Destruction Template

GUIDANCE TO READ BEFORE USING DOCUMENT

- *Purpose* — *This template can be used to record all personal information records that are destroyed.*
- *Responsibility* — *The organisation*
- *Usage* — *The Information Officer and the Deputy Information Officer are the owners of this template. It should be made available to the teams responsible for destruction of records.*

Follow this link to access the template: South Africa GCA Cybersecurity Toolkit - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

Sensitive Information Policy Template

GUIDANCE TO READ BEFORE USING DOCUMENT

- *Purpose* — *This policy should be used by the business as a guide when determining what personal information can be shared with people and/business outside the company.*
- *Responsibility* — *The organisation*
- *Usage* — *By all employees, subsidiaries and third parties related to the organisation*

Follow this link to access the template: South Africa GCA Cybersecurity Toolkit - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

Record of Processing Activities (RoPA) Template

GUIDANCE TO READ BEFORE USING DOCUMENT

- *Purpose* — *This is an inventory of the data processing done by the business. It also provides an overview of all business activities concerning personal data*
- *Responsibility* — *The organisation*
- *Usage* — *Should be used internally by the organisation*

Follow this link to access the template: South Africa GCA Cybersecurity Toolkit - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

Information Security Policy Template

GUIDANCE TO READ BEFORE USING DOCUMENT

- *Purpose* — *This policy should be used as a guide to outline how personal information collected by Company X will be secured and protected*
- *Responsibility* — *The organisation*
- *Usage* — *Should be shared with all employees, subsidiaries and third parties.*

Follow this link to access the template: South Africa GCA Cybersecurity Toolkit - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

Privacy and Information Security Risk Register Template

GUIDANCE TO READ BEFORE USING DOCUMENT

- *Purpose* — *This is a document that record's the company's identified privacy and information security risks , the likelihood and consequences of a risk occurring and the mitigation actions that are being taken to reduce the impact of the risk.*
- *Responsibility* — *The organisation*
- *Usage* — *Should be used internally by the organisation*

Follow this link to access the template: South Africa GCA Cybersecurity Toolkit - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

Opt-In Form Template

GUIDANCE TO READ BEFORE USING DOCUMENT

- *Purpose* — *This template should be used by the Data Subject to record consent to opt-in to direct marketing*
- *Responsibility* — *The Information Officer should be the owner of this template, and responsible for ensuring that this consent is recorded*
- *Usage* — *Should be used shared with the Data Subject.*

Follow this link to access the template: South Africa GCA Cybersecurity Toolkit - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

Opt-Out Form Template

GUIDANCE TO READ BEFORE USING DOCUMENT

- *Purpose* — *This is a form should be made available to the Data Subject. When the Data Subject sets out an opt-out choice, it is recorded against their records and will remain unless the Data Subject changes their mind.*
- *Responsibility* — *The organisation*
- *Usage* — *Should be used shared with the Data Subject*

Follow this link to access the template: South Africa GCA Cybersecurity Toolkit - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

SECTION 04

References

References

1. Information Regulator: https://www.justice.gov.za/inforeg/
2. POPIA: Protection of Personal Information Act (POPI Act) – POPIA
3. SANS Acceptable Use Policy Document: https://sansorg.egnyte.com/dl/fUxcUQSWHn