

PROTECTION OF PERSONAL INFORMATION ACT 4 of 2013
PERSONAL INFORMATION IMPACT ASSESSMENT
MARCH 2025

Foreword

The Promotion of Access to Information Act 2 of 2000 (PAIA) and the Protection of Personal Information Act 4 of 2013 (POPIA) are pieces of legislation used to protect the basic human rights of access to information (PAIA) and privacy (POPIA).

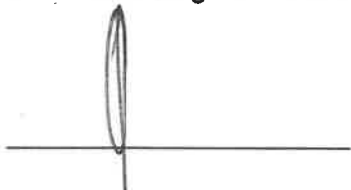
Regulation 4(1) of the 2018 POPIA regulations which came into effect on 1 May 2021, provides for responsibilities of Information Officers. Amongst the responsibilities imposed on Information Officers regulation 4(1)(b) prescribes that Information Officers must ensure that a Personal Information Impact Assessment (PIIA) is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.

Although the legislation requires such a PIIA, little to no guidance is provided in the legislation as to what such an assessment should look like and how it should function.

However, according to training provided by the Information Regulator of South Africa, the identification, assessment and management of privacy risks is a fundamental component of accountability in POPIA. Understanding the risks in which you process personal information is central to an appropriate and proportionate privacy management framework.

A PIIA is therefore an important risk management tool used to enable the identification and recording of personal information and protecting and minimizing the risks.

With this background in mind, the Office of the Premier embarked on compiling this table as a tool to identify and record the personal information processed by it and protecting and minimizing the risks of such personal information.



ANDILE FANI(MR.)

DATE

28/02/2025

HEAD OF DEPARTMENT

DEPARTMENT OF TRANSPORT

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
A. Name and surname; contact details (contact telephone number(s), fax number, email address); residential and postal address; unique identifying number; location information; race; gender; sex; pregnancy; marital status; national, ethnic or social origin; age; physical or mental health; well-being; disability; language; confidential correspondence; education; medical, financial, criminal or employment history.	- Unemployed people in the Eastern Cape - University students (historic and currently registered) in the Eastern Cape - Petitioners to the Office of the Premier - People who are service providers/suppliers - People receiving services from the Office of the Premier and other Departments - People who are recipients of state benefits (e.g. health services, subsidized housing, youth development programmes, etc.)	- Strategic Skills Development and Coordination Unit - Youth Development Unit - Information Communications Technology Unit - Office of the Director-General - IGR & Stakeholder Relations Management - Transformation Programmes	1. Accountability Are there measures in place in order to ensure compliance with the conditions for lawful processing of personal information? (data protection policies, documentation of processing activities, implementation of appropriate security measures). 2. Processing Limitation <u>Lawfulness of processing</u> Is the personal information processed lawfully and in a reasonable manner that does not infringe the privacy of a data subject? <u>Minimality</u> Is the personal information being processed adequate,	- Contractual documentation - Archiving of records - Safe records management processes - ICT security measures - PAIA Manual

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
			relevant and not excessive? <u>Consent, justification and objection</u> Does the responsible party/applicant obtain consent from a data subject when processing personal information? Are there mechanisms in place for data subjects to provide consent for their information to be collected? <u>Collection directly from data subject</u> Is personal Information collected directly from the data subject, except otherwise provided for in section 12(2) of POPIA? 3. Purpose Specification <u>Collection for the specific purpose</u>	

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
			Is the purpose for collection explicitly defined to data subjects? <u>Retention and restriction of records</u> Is there a framework or policy which guides to ensure that data is not kept or retained for any longer than is necessary for achieving the purpose for which the information was collected? Are there guidelines in terms of how personal information is altered, updated, destroyed or deleted? 4. <u>Further Processing</u> <u>Limitation</u> Do you have systems in place to ensure that further processing of personal information is in accordance with the purpose for which it was collected? 5. <u>Information Quality</u>	

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
			Are measures in place to ensure that personal information collected is complete and accurate? 6. <u>Openness</u> Notification of data subject when collecting personal information. Do you inform data subjects that their personal information is being processed (collect, use, storage, distribution, destruction)? Do you inform the data subject of the possible use of their personal information by third parties? If so, under what circumstances? 7. <u>Security Safeguards</u> Security measures on integrity and confidentiality of personal information Are there appropriate measures in place to ensure that the	

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
			integrity and confidentiality of personal information is secured? Have regular verifications been conducted to assess if the safeguards are effectively implemented? Do you continually update safeguard mechanisms in response to new risks or deficiencies? <u>Notification of security compromises</u> Are there procedures in place to inform the information officer of a notifiable breach or personal security compromise? 8. <u>Data Subject Participation</u> <u>Access to personal information</u> Is there a system in place to grant data subjects easy access to their personal information?	

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
			<u>Correction of personal information</u> Are there procedures in place to correct or delete personal information about the data subject that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully?	
B. Names of contact persons; name of legal entity; physical and postal address; contact details (contact number(s), fax number, email address); registration number; financial, commercial, scientific or technical information.	1. Registered trusts, close corporations, and companies that contract with OTP 2. Petitioners to the Office of the Premier	1. Strategic Skills Development and Coordination Unit 2. Youth Development Unit 3. Information Communications Technology Unit 4. Supply Chain Management in procurement processes. 5. Information Communications Technology Unit 6. Office of the Director-General	1. <u>Accountability</u> Are there measures in place to ensure compliance with the conditions for lawful processing of personal information? (data protection policies, documentation of processing activities, implementation of appropriate security measures). 2. <u>Processing Limitation</u> Lawfulness of processing	1. Contractual documentation 2. Archiving of records 3. Safe records management processes 4. ICT security measures

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
		7. IGR & Stakeholder Relations Management 8. Office of the Chief State Law Advisor	Is the personal information processed lawfully and in a reasonable manner that does not infringe the privacy of a data subject? <u>Minimality</u> Is the personal information being processed adequate, relevant and not excessive? <u>Consent, justification and objection</u> Does the responsible party/applicant obtain consent from a data subject when processing personal information? Are there mechanisms in place for data subjects to provide consent for their information to be collected? <u>Collection directly from data subject</u> Is personal Information collected directly from the data	

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
			subject, except otherwise provided for in section 12(2) of POPIA? 3. <u>Purpose</u> <u>Specification</u> Collection for the <u>specific purpose</u> Is the purpose for collection explicitly defined to data subjects? <u>Retention and restriction of records</u> Is there a framework or policy which guides to ensure that data is not kept or retained for any longer than is necessary for achieving the purpose for which the information was collected? Are there guidelines in terms of how personal information is altered, updated, destroyed or deleted? 4. <u>Further Processing</u> <u>Limitation</u>	

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
			Do you have systems in place to ensure that further processing of personal information is in accordance with the purpose for which it was collected? 5. <u>Information Quality</u> Are measures in place to ensure that personal information collected is complete and accurate? 6. <u>Openness</u> Notification of data subject when collecting personal information. Do you inform data subjects that their personal information is being processed (collect, use, storage, distribution, destruction)? Do you inform the data subject of the possible use of their personal information by third parties? If so, under what circumstances?	

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
			7. Security Safeguards <u>Security measures on integrity and confidentiality of personal information</u> Are there appropriate measures in place to ensure that the integrity and confidentiality of personal information is secured? Have regular verifications been conducted to assess if the safeguards are effectively implemented? Do you continually update safeguard mechanisms in response to new risks or deficiencies? <u>Notification of security compromises</u> Are there procedures in place to inform the information officer of a notifiable breach or personal security compromise?	

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
			8. Data Subject Participation <u>Access to personal information</u> Is there a system in place to grant data subjects easy access to their personal information? <u>Correction of personal information</u> Are there procedures in place to correct or delete personal information about the data subject that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully?	
C. Gender, pregnancy; marital status; race; age, language, educational information (qualifications); financial information; employment history; ID number; physical and postal address;	Employees and prospective employees	1. Human Resource Management 2. Integrity and Security Management 3. Service providers (e.g. Employee Wellness services)	1. Accountability Are there measures in place to ensure compliance with the conditions for lawful processing of personal information? (data protection policies, documentation of	1. Contractual documentation 2. Archiving of records 3. Safe records management processes 4. ICT security measures

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
contact details (contact number(s), fax number, email address); criminal behaviour; well-being and their relatives (family members); race; medical; gender; sex; nationality; ethnic or social origin; sexual orientation; age; physical or mental health; well-being; disability; religion; conscience; belief; culture; language; biometric information of the person as is required in public service prescripts and policies.		4. Information Communications Technology Unit 5. Office of the Chief State Law Advisor	processing activities, implementation of appropriate security measures). 2. Processing Limitation <u>Lawfulness of processing</u> Is the personal information processed lawfully and in a reasonable manner that does not infringe the privacy of a data subject? <u>Minimality</u> Is the personal information being processed adequate, relevant and not excessive? <u>Consent, justification and objection</u> Does the responsible party/applicant obtain consent from a data subject when processing personal information? Are there mechanisms in place for data subjects to	

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
			provide consent for their information to be collected? <u>Collection directly from data subject</u> Is personal Information collected directly from the data subject, except otherwise provided for in section 12(2) of POPIA? 3. <u>Purpose</u> <u>Specification</u> Collection for the <u>specific purpose</u> Is the purpose for collection explicitly defined to data subjects? <u>Retention and restriction of records</u> Is there a framework or policy which guides to ensure that data is not kept or retained for any longer than is necessary for achieving the purpose for which the information was collected?	

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
			Are there guidelines in terms of how personal information is altered, updated, destroyed or deleted? 4. <u>Further Processing Limitation</u> Do you have systems in place to ensure that further processing of personal information is in accordance with the purpose for which it was collected? 5. <u>Information Quality</u> Are measures in place to ensure that personal information collected is complete and accurate? 6. <u>Openness</u> Notification of data subject when collecting personal information. Do you inform data subjects that their personal information is being processed (collect, use, storage, distribution, destruction)?	

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
			Do you inform the data subject of the possible use of their personal information by third parties? If so, under what circumstances? 7. <u>Security Safeguards</u> <u>Security measures on integrity and confidentiality of personal information</u> Are there appropriate measures in place to ensure that the integrity and confidentiality of personal information is secured? Have regular verifications been conducted to assess if the safeguards are effectively implemented? Do you continually update safeguard mechanisms in response to new risks or deficiencies? <u>Notification of security compromises</u>	

<u>PERSONAL INFORMATION PROCESSING</u>	<u>DATA SUBJECTS</u>	<u>WHO IS INVOLVED</u>	<u>COMPLIANCE WITH 8 POPIA PRINCIPLES</u>	<u>MITIGATION MEASURES</u>
			Are there procedures in place to inform the information officer of a notifiable breach or personal security compromise? 8. <u>Data Subject Participation</u> <u>Access to personal information</u> Is there a system in place to grant data subjects easy access to their personal information? <u>Correction of personal information</u> Are there procedures in place to correct or delete personal information about the data subject that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully?	