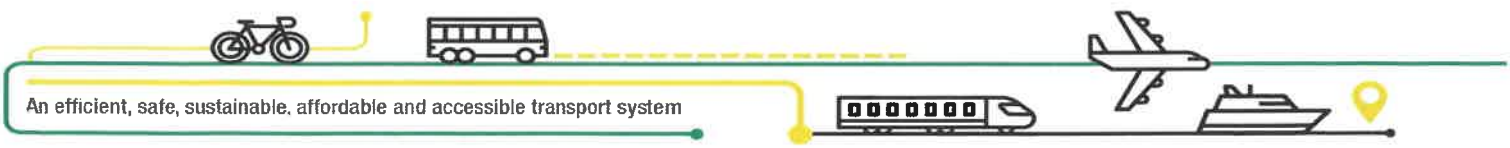
PROTECTION OF PERSONAL INFORMATION ACT 4 of 2013

PERSONAL INFORMATION IMPACT ASSESSMENT

MARCH 2026/2027



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 PAIA 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 Department of Transport embarked on compiling this table as a tool to identify and record the personal information processed by it and protecting and minimize the risks of such personal information.

Andile Fani

Signed by Andile Fani, Andile.Fani@ectransport.gov.za
10/06/2026 15:24:54(UTC+02:00) SIGNIFLOW

ANDILE FANI (MR.)
HEAD OF DEPARTMENT
DEPARTMENT OF TRANSPORT

DATE

PERSONAL INFORMATION PROCESSING	DATA SUBJECTS	WHO IS INVOLVED	COMPLIANCE WITH 8 POPIA PRINCIPLES	MITIGATION MEASURES
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.	1. Unemployed people in the Eastern Cape 2. University students (historic and currently registered) in the Eastern Cape 3. Petitioners to the Department of Transport 4. People who are service providers/suppliers 5. People receiving services from the Department of Transport and other Departments 6. People who are recipients of state benefits (e.g. health services, subsidized housing, youth development programmes, etc.)	1. Strategic Skills Development and Coordination Unit 2. Youth Development Unit 3. Information Communications Technology Unit 4. IGR & Stakeholder Relations Management 5. 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** Lawfulness of processing Is the personal information processed lawfully and in a reasonable manner that does not infringe the privacy of a data subject? Minimality Is the personal information being processed adequate,	1. Contractual documentation 2. Archiving of records 3. Safe records management processes 4. ICT security measures 5. PAIA Manual

			relevant and not excessive? Consent, justification and objection 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? Collection directly from data subject Is personal Information collected directly from the data subject, except otherwise provided for in section 12(2) of POPIA? **3. Purpose Specification** Collection for the specific purpose Is the purpose for collection explicitly defined to data subjects?	

			Retention and restriction of records 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. **Further Processing Limitation** 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. **Information Quality** Are measures in place to ensure that personal information collected is complete and accurate? 6. **Openness** 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. **Security Safeguards** Security measures on integrity and confidentiality of personal information 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? Notification of security compromises Are there procedures in place to inform the information officer of a notifiable breach or personal security compromise? 8. **Data Subject Participation** Access to personal information Is there a system in place to grant data subjects easy access to their personal information? Correction of personal information 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;	1. Registered trusts, close corporations, and companies that contract with	1. Strategic Skills Development and Coordination Unit	**1. Accountability** Are there measures in place to ensure compliance with the	1. Contractual documentation 2. Archiving of records

contact details (contact number(s), fax number, email address); registration number; financial, commercial, scientific or technical information.	Department of Transport 2. Petitioners to the Office of the Premier	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 Head of Department 7. Legal Services Directorate	conditions for lawful processing of personal information? (data protection policies, documentation of processing activities, implementation of appropriate security measures). **2. Processing Limitation** Lawfulness of processing Is the personal information processed lawfully and in a reasonable manner that does not infringe the privacy of a data subject? Minimality Is the personal information being processed adequate, relevant and not excessive? Consent, justification and objection Does the responsible party/applicant obtain consent from a data subject when processing personal information?	3. Safe records management processes 4. ICT security measures

			Are there mechanisms in place for data subjects to provide consent for their information to be collected? Collection directly from data subject Is personal Information collected directly from the data subject, except otherwise provided for in section 12(2) of POPIA? **3. Purpose Specification** Collection for the specific purpose Is the purpose for collection explicitly defined to data subjects? Retention and restriction of records 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. **Further Processing Limitation** 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. **Information Quality** Are measures in place to ensure that personal information collected is complete and accurate? 6. **Openness** 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. **Security Safeguards** Security measures on integrity and confidentiality of personal information 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? Notification of security compromises Are there procedures in place to inform the information officer of a notifiable breach or personal security compromise? 8. **Data Subject Participation**	

			Access to personal information Is there a system in place to grant data subjects easy access to their personal information? Correction of personal information 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; contact details (contact number(s), fax number, email address); criminal behaviour; well-being and their relatives	Employees and prospective employees	1. Human Resource Management 2. Integrity and Security Management 3. Service providers (e.g. Employee Wellness services) 4. Information Communications Technology Unit 5. Legal Services Directorate	1. **Accountability** 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. **Processing Limitation**	1. Contractual documentation 2. Archiving of records 3. Safe records management processes 4. ICT security measures

(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.			Lawfulness of processing Is the personal information processed lawfully and in a reasonable manner that does not infringe the privacy of a data subject? Minimality Is the personal information being processed adequate, relevant and not excessive? Consent, justification and objection 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? Collection directly from data subject Is personal Information collected directly from the data subject, except otherwise provided for	

			in section 12(2) of POPIA? 3. **Purpose Specification** Collection for the specific purpose Is the purpose for collection explicitly defined to data subjects? Retention and restriction of records 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. **Further Processing Limitation** 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. **Information Quality** Are measures in place to ensure that personal information collected is complete and accurate? 6. **Openness** 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. **Security Safeguards** Security measures on integrity and confidentiality of personal information 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? Notification of security compromises Are there procedures in place to inform the information officer of a notifiable breach or personal security compromise? 8. **Data Subject Participation** Access to personal information Is there a system in place to grant data subjects easy access to their personal information? Correction of personal information 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?	