Province of the
EASTERN CAPE
TRANSPORT

PROTECTION OF PERSONAL INFORMATION ACT 4 of 2013

COMPLIANCE FRAMEWORK

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)(a) prescribes that Information Officers must ensure that a compliance framework is developed, implemented, monitored and maintained.

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

However, according to training provided by the Information Regulator of South Africa, a compliance framework provides a framework which provides a holistic overview of how an organisation creates and manages its enterprise-wide information assets (records, personal information and data) within the regulatory environment. Furthermore, the Information Regulator indicates that a Compliance Framework will support the fundamentals of an effective privacy management programme and that it will comprise of all the strategies, initiatives, policies, procedures, standards and guidelines that work collectively to achieve POPIA compliance.

With this background in mind, the Office of the Premier embarked on compiling this table as evidence of the development, implementation, monitoring and maintenance of its POPIA Compliance Framework.

28/02/2025

ANDILE FANI (MR.) **DATE**

HEAD OF DEPARTMENT

DEPARTMENT OF TRANSPORT

A.	ESTABLISHING A GOVERNANCE FRAMEWORK		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
1.	Register the Information Officer (IO)/Designate or Delegate a Deputy Information Officer/S if required.	Yes	Review annually
2.	IO to develop a compliance framework.	Yes	Review annually
3.	Conduct a personal information impact assessment to determine adequate technical and organisational and measures are put in place.	Yes	Review annually

A.	ESTABLISHING A GOVERNANCE FRAMEWORK		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
4.	Ensure that there is a PAIA manual (S14 PAIA Act).	Yes	Review annually
5.	Internal measures are developed together with adequate systems to process requests for information or access.	Yes	Review annually
6.	Conduct internal awareness sessions on POPIA, regulations, codes of conduct or information issued by the Regulator.	Yes	Review annually

A.	ESTABLISHING A GOVERNANCE FRAMEWORK		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
7.	Ensure that an Organisational Structure clearly identifies operational roles.	Yes	Review annually
8.	Develop Policies and Procedures to give effect to the governance structure.	Yes	Review annually
9.	Ensure that there is a Review Process of all Policies and Procedures.	Yes	Review annually

B.	RISK ASSESSMENT		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
1.	Integrate the protection of personal information with risk assessments and risk reporting.	In progress	In progress
2.	Undertake an assessment of all processing activities undertaken per division and assess the risks and risk reporting required	In progress	In progress
3.	Identify risks and identify mitigating measures linked to each processing activity.	In progress	In progress

C.	RECORDS MANAGEMENT		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
1.	Develop a records management policy which must incorporate the following:		
1.1.	Identify what is a record?	Yes	Review annually
1.2.	Identify records that require additional protection.	Yes	Review annually
1.3.	Retention and disposal periods must be identified.	Yes	Review annually

C.	RECORDS MANAGEMENT		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
1.4.	Identify where records will be stored.	Yes	Review annually
1.5.	Assign individuals to implement the records management policy, tools and implementation plan	Yes	Review annually
1.6.	Train staff on information that is to be retained and that which should be disposed of.	Yes	Review annually
1.7.	Develop an electronic records and document management system (ERDMS).	Yes	Review regularly

C.	RECORDS MANAGEMENT		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
1.8.	The ERDMS must enable access of certain categories of information to select employees, segregate duties to enhance protection of personal information.	Yes	Review regularly
1.9.	Maintain a register of all employees and their corresponding access to information technology systems and records.	Yes	Review regularly
2.	Developing a disaster management and recovery plan and a business continuity policy. Identify personal information and records that need to be backed up.	Yes	Review regularly
3.	Store backups of electronic information and systems offsite.	Yes	Review regularly

C.	RECORDS MANAGEMENT		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
4.	Secure Storage, Personal information must be stored securely to prevent unauthorised access.	Yes	Review regularly

D.	DEVELOP AN INTERNAL POLICY ON THE PROTECTION OF PERSONAL INFORMATION		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
1.	The policy must guide the organisation, its employees on how to process personal information and align with the conditions for lawful processing and must incorporate the following:	In progress	In progress
2.	Develop a protection of personal information strategy.	In progress	In progress
3.	Develop a protection of personal information charter	In progress	In progress
4.	Include protection of personal information in the mission, values and culture of organisation.	In progress	In progress

D.	DEVELOP AN INTERNAL POLICY ON THE PROTECTION OF PERSONAL INFORMATION		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
5.	Require employees to acknowledge and agree to adhere to the protection of personal information/ privacy policies in writing.	In progress	In progress
6.	Conduct an annual review of the policy	In progress	In progress
7.	Incorporate principles of ethical governance of personal information.	In progress	In progress
8.	Undertake an assessment of all processing activities undertaken per division.	In progress	In progress

D.	DEVELOP AN INTERNAL POLICY ON THE PROTECTION OF PERSONAL INFORMATION		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
9.	Each processing activity must be identified in terms of the relevant division, job function.	In progress	In progress
10.	Identify if there is compliance with POPIA in relation to each processing activity.	In progress	In progress
11.	Assign individuals to implement the records management policy, tools and implementation plan.	Yes	Review annually
12.	Categorise the different types of information that is being processed (Personnel, Legal, Financial, Disaster Recovery, Commercial, and Operational).	Yes	Review annually

D.	DEVELOP AN INTERNAL POLICY ON THE PROTECTION OF PERSONAL INFORMATION		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
13.	Develop an inventory of personal information.	In progress	In progress
14.	Record all processing Activities and maintain a register of each processing activity.	In progress	In progress
15.	Develop a system to classify information and develop a retention and disposal policy in accordance with each data set, category of personal information.	In progress	In progress
16.	Conduct an audit of all current processes that collect, store, share, correct and delete personal information.	In progress	In progress

D.	DEVELOP AN INTERNAL POLICY ON THE PROTECTION OF PERSONAL INFORMATION		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
17.	Identify special personal information	In progress	In progress
18.	Identify all personal information that is processed	In progress	In progress
19.	Identify how personal information is collected	In progress	In progress
20.	Identify where personal information is collected, stored and processed	In progress	In progress

D.	DEVELOP AN INTERNAL POLICY ON THE PROTECTION OF PERSONAL INFORMATION		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
21.	Identify each person that processes personal information	In progress	In progress
22.	Maintain a register of every activity conducted and its associated processing activity	In progress	In progress
23.	Develop a procedure to enable the data subject to object to the processing of their personal information.(Section 11)	Yes	Review annually
24.	Develop a policy on record retention.(Section 14)	Yes	Review annually

D.	DEVELOP AN INTERNAL POLICY ON THE PROTECTION OF PERSONAL INFORMATION		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
25.	Develop a policy on information quality to ensure that information is updated and accurate	In progress	In progress
26.	Develop a procedure to deal with the correction and deletion of personal information.	Yes	Review annually
27.	Develop a process to notify the data subject on the reason for processing, the type of information that is being processed, the details of the responsible party processing the personal information, if the necessary consent was secured, was the personal information collected directly from the data subject.	In progress	In progress
28.	Conduct a process to map all personal information processing	In progress	In progress

D.	DEVELOP AN INTERNAL POLICY ON THE PROTECTION OF PERSONAL INFORMATION		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
29.	Ensure that the personal information mapping process is reviewed on a regular basis	In progress	In progress
30.	Establish a lawful basis for all processing of personal information	Yes	Review annually
31.	Develop a framework to establish and assess legitimate interest	In progress	In progress
32.	Document the lawful basis for processing of personal information	In progress	In progress

D.	DEVELOP AN INTERNAL POLICY ON THE PROTECTION OF PERSONAL INFORMATION		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
33.	Establish a register of all consents that have been secured	No	