agriculture

Department:
Agriculture
PROVINCE OF THE EASTERN CAPE

PROTECTION OF PERSONAL INFORMATION ACT 4 of 2013

COMPLIANCE FRAMEWORK

APRIL 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 organization 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 Department of Agriculture embarked on compiling this table as evidence of the development, implementation, monitoring and maintenance of its POPIA Compliance Framework.

MR B. DAYIMANI
HEAD OF DEPARTMENT
DEPARTMENT OF AGRICULTURE

18.06.2025

DATE

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.	Information Officers to develop a compliance framework.	Yes	Review annually
3.	Conduct a personal information impact assessment to determine adequate technical and organizational and measures are put in place.	Yes	Review annually
4.	Ensure that there is a PAIA manual (S14 PAIA Act).	Yes	Review annually

A.	ESTABLISHING A GOVERNANCE FRAMEWORK		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
5.	Internal measures are developed together with adequate systems to process requests for information or access.	yes	POPIA notices to change/ update / delete personal information are available on the website. All requests for information (HR, SCM, farmer support, training requirements) are preceded by a POPIA notice.
6.	Conduct internal awareness sessions on POPIA, regulations, codes of conduct or information issued by the Regulator.	In progress	Actioned
7.	Ensure that an Organizational Structure clearly identifies operational roles.	Yes	Review every 5 years annually
8.	Develop Policies and Procedures to give effect to the governance structure.	Yes	Review every 3 years annually

A.	ESTABLISHING A GOVERNANCE FRAMEWORK		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
9.	Ensure that there is a Review Process of all Policies and Procedures.	Yes	Review every 3 years
10.	Develop an inventory and process flow chart of the location of all personal information being processed.	In Progress	A communique to all Chief Directors to develop an inventory list of all personal information processed within the programme and location of same. These inventory lists to be stored by Records Management

B.	RISK ASSESSMENT		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
1.	Integrate the protection of personal information with risk assessments and risk reporting. Identified risk and mitigation measures are linked to each processing activity.	Yes	Reviewed annually
2.	Undertake an assessment of all processing activities undertaken per division and assess the risks and risk reporting required	yes	Reviewed every 2 years
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.	Review a records management policy which must incorporate the following:	Yes	Review every 3 years annually
1.1.	Identify what is a record?	Yes	Completed
1.2.	Identify records that require additional protection, 1. HOD 2. MEC 3. LABOUR RELATIONS 4. SECURITY CLASIFIFACTION	In progress	Review annually
1.3.	Retention schedule and disposal periods must be identified. 1. Training officials from various Directorates on understanding the provisions of the manual and electronic systems	Yes	Review annually
1.4.	Identify where records will be stored. 1. Current records (active-records) 2. Non-Current records (in-active records)	In progress	Review annually

C.	RECORDS MANAGEMENT		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
1.5.	Assign individuals to implement the records management policy, tools and implementation plan 1. Appoint (nominate) Records Management Champions 2. Set aside Records Management Day 3. Utilize big screens on foyers which will encourage the entire work force of DRDAR to adhere to Records Management policy and guidelines	Yes	Review annually
1.6.	Train staff on information that is to be retained and that which should be disposed of (same as retention periods)	In progress	Review annually
1.7.	Develop an electronic records and document management system (ERDMS). 1. IT will play a pivotal role in developing the ERDMS in phases	Yes	Completed.
1.8.	The ERDMS must enable access of certain categories of information to select employees, segregate duties to enhance protection of personal information.	Yes	Reviewed annually with new appointments.
1.9.	Maintain a register of all employees and their corresponding access to information technology systems and records.	In progress	Review annually

C.	RECORDS MANAGEMENT		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
2.	Developing a disaster management and recovery plan and a business continuity policy. Identify personal information and records that need to be backed up. 1. A collaborative approach by the following units, Records Management, ICT, Risk and Disaster Management are playing an important role in developing the above mentioned plan	In progress	Review 3 years
3.	Store backups of electronic information and systems offsite. 1. The Departmental ICT Unit should develop a back-up system for records should any disaster affect the institutional memory adversely.	Yes	Reviewed regularly
4.	Secure Storage, Personal information must be stored securely to prevent unauthorized access.	Yes	Reviewed 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:	Yes	Review every 3 years
2.	Develop a protection of personal information strategy.	Yes	Review every 3 years
3.	Require employees to acknowledge and agree to adhere to the protection of personal information/ privacy policies in writing.	Yes	Review regularly
4.	Conduct review of the policy	Yes	Every 3 years

D.	DEVELOP AN INTERNAL POLICY ON THE PROTECTION OF PERSONAL INFORMATION		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
5.	Incorporate principles of ethical governance of personal information.	Yes	
6.	Undertake an assessment of all processing activities undertaken per division: • Each processing activity must be identified in terms of the relevant division, job function. • Identify if there is compliance with POPIA in relation to each processing activity. • All processes that collect, store, process personal information.	In progress	Every 3 years
7.	Assign individuals to implement the records management policy, tools and implementation plan.	Yes	Review every 3 years
8.	Categorise the different types of information that is being processed (Personnel, Legal, Financial, Disaster Recovery, Commercial, and Operational).	Yes	Review every 3 years

D.	DEVELOP AN INTERNAL POLICY ON THE PROTECTION OF PERSONAL INFORMATION		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
9.	Develop a procedure to enable the data subject to object to the processing of their personal information (Section 11)	Yes	POPIA form1 and 2 available on website for objection to processing of personal information/ correction/ deletion of personal information.
10.	Develop a policy on record retention (Section 14) (retention periods done by records management section).	Yes	Review every 3 years
11.	Develop a policy on information quality to ensure that information is updated and accurate	Yes	Review every 3 years
12.	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.	Yes	Generic consent form developed and available for all DOA data subjects.
13.	Establish a lawful basis for all processing of personal information and document the lawful basis for processing of personal information.	Yes	Review annually

D.	DEVELOP AN INTERNAL POLICY ON THE PROTECTION OF PERSONAL INFORMATION		
	Task	**Completed: Yes/No/In progress**	**Review/Action**
14.	Develop a framework to establish and assess legitimate interest	In progress	Review every 3 years
15.	Establish a register of all consents that have been secured	Yes	Annually

REVIEWED:

MR B. DAYIMANI
HOD
DATE: 25 JUNE 2025