

## ECDSD POPIA IMPACT ASSESSMENT REPORT

### The Objectives of the POPIA Impact Assessment

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.

### **The approach used to conduct the impact assessment**

- Interviews and Questionnaires were used to gather data from different programmes/branches and District offices.
- Site inspection to different offices was used to verify and the collect the secondary data
- Verification of personal information based on data collection tools used by the individual programme/office

### **Participants**

Participants to the assessments were Programme 1(branches), programme 2, programme 3, programme 4, programme 5, and all Districts

### **Focus areas of assessment**

The assessment tool has categorized the gathered information as follows:

- Personal information processed by the individual office (district office, institution or head office) or branch or programme within the Department;
- The categories of data subjects involved in the process of data processing by the Department;
- The individual office/branch/programme (district office, institution or head office) representing the Department in processing the personal information.
- An Identified compliance gaps against POPIA principles that needs to be addressed by management

- Recommended control measures by the Department based on the identified POPIA compliance gaps

### Key threats identified to POPIA Compliance

- Compromised security of records in different offices/programs due to lack of secured storage facilities.
- Shortage of storage space for records due to noncompliance to records lifecycle management and lack of records management strategy.
- Data collection tools with no consent statement
- Lack of standardized contract statement in relation to personal information

### Assessment outcomes and action plan

The Office/branch	(Both PI and SPI) Personal information processed by the individual office and means of Verification	Categories of data subjects	Identified compliance gaps against POPIA principles (P refer to principle- and then number)	Recommended control measures
-------------------	--	-----------------------------	---	------------------------------

<p>Corporate services branch</p>	<p>Surname, names, DOB, ID, address, contact numbers, Qualifications, race, gender, pregnancy, marital, status, national, ethnic or social origin, colour, gender, disability, language, criminal, employment history, fingerprinting, pay point, date of employment, previous employer</p> <p>Means of verification were done through Z83, PERSAL report and Security vetting forms, HRMS, security visitors attendance register, Personal file</p>	<p>Applicants, employees, service providers. Contract workers, interns</p>	<p>No guidance documents on PI (policies &amp; procedures therefore in violation of P1, P2. No consent for further sharing PI therefore in violation with P4. No Quality controls and constant update of PI therefore in violation with P5. Data subject is notified of on possible sharing PI with 3<sup>rd</sup> party therefore in compliance with P6 Most of the documents are store in a non-lockable cabinets, boxes, shelves and unlocked offices. This is compromising the security control measures of ensuring confidentiality, integrity, and security of PI therefore there is no compliance with P7 Processes are in place to allow data subject to update PI therefore in compliance with P8</p>	<ol style="list-style-type: none"> <li>1. Employees should be educated on Security breach procedure after it has been amended to incorporate PI</li> <li>2. Everyone within the supervision of the individual office/branch/programme should understand the implications of POPIA in her/his process.</li> <li>3. Policy guiding framework should developed to guide the entire Department.</li> <li>4. Further Processing of PI should be accompanied by a standardized Departmental consent statement.</li> <li>5. CFO branch should issue a statement to all their data subjects in relation to POPIA as required in P 5, P6 and P8.</li> <li>6. All data collection/processing tools should be used after a Departmental/National consent statement.</li> <li>7. Data collection tools should have a Departmental disclaimer in relation to PI processing.</li> <li>8. Review of records management and information management policy to include POPIA compliance requirements and measures.</li> <li>9. Review of Departmental physical storage facilities and including offices with PI information to be more secured with locks, and lockable storage facilities or digitized.</li> <li>10. Update Corporate risk register to include PI storage.</li> <li>11. Apply for a prior authorization from Information Regulator for historical PI and SPI</li> <li>12.</li> </ol>
----------------------------------	--	--	--	---



Province of the  
**EASTERN CAPE**

<p>Chief Information Officer branch</p>	<p>Surname, names, Persal No, office telephon/ cell number, fax, email address, job title, rank, office identification Means of verification: ICT forms for service application and support such Training Nomination and Access Request Application IT equipment, network form, active director for e-mail services, VPNra application, BAS application form/ PERSAL application Form, HRMS Change Control Form, Procure to Pay(P2P) Amendment Form, Systems Password Reset Form</p>	<p>Employees, auditors, contract workers, interns</p>	<p>No guidance documents on PI (policies &amp; procedures therefore in violation of P1, P2. No consent for further sharing PI therefore in violation with P4. No Quality controls and constant update of PI therefore in violation with P5. Data subject is notified of on possible sharing PI with 3<sup>rd</sup> party therefore in compliance with P6 Most of the documents are store in a non-lockable cabinets, boxes, shelves and unlocked offices. This is compromising the security control measures of ensuring confidentiality, integrity, and security of PI therefore there is no compliance with P7.  Processes are in place to allow data subject to update PI therefore in compliance with P8</p>	<ol style="list-style-type: none"><li>1. Employees should be educated on Security breach procedure after it has been amended to incorporate PI</li><li>2. Everyone within the supervision of the individual office/branch/programme should be understand the implications of POPIA in her/his proceses.</li><li>3. Policy guiding framework should developed to guide the entire Department.</li><li>4. Further Processing of PI should be accompanied by a standardized Departmental consent statement.</li><li>5. ICT branch should issue a statement to all their data subjects in relation to POPIA as required in P 5, P6 and P8.</li><li>6. All data collection/processing tools should be used after a Departmental/National consent statement.</li><li>7. Data collection tools should have a Departmental disclaimer in relation to PI processing.</li><li>8. Review of records management and information management policy to include POPIA compliance requirements and measures</li><li>9. Review of Departmental physical storage facilities and including offices with PI information to be more secured with locks, and lockable storage facilities or digitized</li><li>10. Update Corporate risk register to include PI storage</li></ol>
---	--	---	--	--



Province of the  
**EASTERN CAPE**

<p>Chief financial officer branch</p>	<p>Surname, names, address, telephone number, fax number, cell phone no, email address, ID no, bank details, company name, tax details, company registration number, vat reg-no, names directors, color, gender, witness surname and name, B-BBEE STATUS LEVEL country of origin, bid price, persal no, supplier number, NPO registration number, NPO name,</p> <p>Means of PI verification: SBD forms, CSD database/forms, BAS entity form, attendance register</p>	<p>NPOs, Suppliers, employees, contractors, auditors, audit committee members</p>	<p>No guidance documents on PI (policies &amp; procedures therefore in violation of P1, P2. With suppliers there is current control of getting a consent but in other data subjects there is No consent for further sharing PI therefore in violation with P4. No Quality controls and constant update of PI therefore in violation with P5. Data subject is notified of on possible sharing PI with 3<sup>rd</sup> party therefore in compliance with P6</p> <p>Most of the documents are store in a non-lockable cabinets, boxes, shelves and unlocked offices. This is compromising the security control measures of ensuring confidentiality, integrity, and security of PI therefore there is no compliance with P7.</p> <p>Processes are in place to allow data subject to update PI therefore in compliance with P8</p>	<ol style="list-style-type: none"> <li>1. Employees should be educated on Security breach procedure after it has been amended to incorporate PI</li> <li>2. Everyone within the supervision of the individual office/branch/programme should be understand the implications of POPIA in her/his proceses.</li> <li>3. Policy guiding framework should developed to guide the entire Department.</li> <li>4. Further Processing of PI should be accompanied by a standardized Departmental consent statement.</li> <li>5. CFO branch should issue a statement to all their data subjects in relation to POPIA as required in P 5, P6 and P8.</li> <li>6. All data collection/processing tools should be used after a Departmental/National consent statement.</li> <li>7. Data collection tools should have a Departmental disclaimer in relation to PI processing.</li> <li>8. Review of records management and information management policy to include POPIA compliance requirements and measures</li> <li>9. Review of Departmental physical storage facilities and including offices with PI information to be more secured with locks, and lockable storage facilities or digitized</li> <li>10. Update Corporate risk register to include PI storage</li> </ol>
---------------------------------------	--	---	--	---





<p>Programme 2</p>	<p>Surname, names Residential, postal address; ID number; location information; race, gender, sex; pregnancy, marital status, national, ethnic, age, physical or mental health, well-being, disability status, language, confidential correspondence; education; medical, financial, employment history, income status, HIV /AIDS Status, guardian, parents details, next of kin details</p> <p>Means of PI verification: SRD form, Social work forms, NISIS data, Community based information system, Older person register, attendance register, NPO facilities system, NPO registration forms.</p>	<p>NPOs, Suppliers, employees, , older persons, house hold headed by children, community members, parents and Guardian</p>	<p>No guidance documents on PI (policies &amp; procedures therefore in violation of P1, P2. With suppliers there is current control of getting a consent but in other data subjects there is No consent for further sharing PI therefore in violation with P4. No Quality controls and constant update of PI therefore in violation with P5. Data subject is notified of on possible sharing PI with 3<sup>rd</sup> party therefore in compliance with P6 Most of the documents are store in a non-lockable cabinets, boxes, shelves and unlocked offices. This is compromising the security control measures of ensuring confidentiality, integrity, and security of PI therefore there is no compliance with P7. Processes are in place to allow data subject to update PI therefore in compliance with P8</p>	<ol style="list-style-type: none"> <li>1. Employees should be educated on Security breach procedure after it has been amended to incorporate PI</li> <li>2. Everyone within the supervision of the individual office/branch/programme should be understand the implications of POPIA in her/his process.</li> <li>3. Policy guiding framework should developed to guide the entire Department.</li> <li>4. Further Processing of PI should be accompanied by a standardized Departmental consent statement.</li> <li>5. CFO branch should issue a statement to all their data subjects in relation to POPIA as required in P 5, P6 and P8.</li> <li>6. All data collection/processing tools should be used after a Departmental/National consent statement.</li> <li>7. Data collection tools should have a Departmental disclaimer in relation to PI processing.</li> <li>8. Review of records management and information management policy to include POPIA compliance requirements and measures</li> <li>9. Review of Departmental physical storage facilities and including offices with PI information to be more secured with locks, and lockable storage facilities or digitized.</li> <li>10. Update Corporate risk register to include PI storage</li> </ol>
--------------------	---	--	--	---

<p>Programme 3</p>	<p>Surname, names Residential, postal address; ID number; location information; race, gender, sex; pregnancy, marital status, national, ethnic, age, physical or mental health, well-being, disability status, language, confidential correspondence; education; medical, financial, employment history, income status, HIV /AIDS Status, guardian, parents details, next of kin details, perpetrator details</p> <p>Means of PI verification: Foster care register form, Child protection registration form/system, Social work forms, NISIS data, adoption forms/register, attendance register, NPO facilities system, NPO registration forms.</p>	<p>NPOs, Suppliers, employees, parents, guardian, household members, children clients, family</p>	<p>No guidance documents on PI (policies &amp; procedures therefore in violation of P1, P2. With suppliers there is current control of getting a consent but in other data subjects there is No consent for further sharing PI therefore in violation with P4. No Quality controls and constant update of PI therefore in violation with P5. Data subject is notified of on possible sharing PI with 3<sup>rd</sup> party therefore in compliance with P6 Most of the documents are store in a non-lockable cabinets, boxes, shelves and unlocked offices. This is compromising the security control measures of ensuring confidentiality, integrity, and security of PI therefore there is no compliance with P7. Processes are in place to allow data subject to update PI therefore in compliance with P8</p>	<ol style="list-style-type: none"> <li>1. Employees should be educated on Security breach procedure after it has been amended to incorporate PI</li> <li>2. Everyone within the supervision of the individual office/branch/programme should be understand the implications of POPIA in her/his process.</li> <li>3. Policy guiding framework should developed to guide the entire Department.</li> <li>4. Further Processing of PI should be accompanied by a standardized Departmental consent statement.</li> <li>5. CFO branch should issue a statement to all their data subjects in relation to POPIA as required in P 5, P6 and P8.</li> <li>6. All data collection/processing tools should be used after a Departmental/National consent statement.</li> <li>7. Data collection tools should have a Departmental disclaimer in relation to PI processing.</li> <li>8. Review of records management and information management policy to include POPIA compliance requirements and measures</li> <li>9. Review of Departmental physical storage facilities and including offices with PI information to be more secured with locks, and lockable storage facilities or digitized.</li> <li>10. Update Corporate risk register to include PI storage</li> </ol>
--------------------	--	---	--	---



<p>Programme 4</p>	<p>Surname, names Residential, postal address; ID number; location information; race, gender, sex; pregnancy, marital status, national, ethnic, age, physical or mental health, well-being, disability status, language, confidential correspondence; education; medical, financial, employment history, income status, HIV /AIDS Status, guardian, parents details, next of kin details</p> <p>Means of PI verification: Probation case management form/system, Child youth care facility registration forms/system, Victim empowerment register/information system, rehabilitation register, subsistence abuse client register</p>	<p>NPOs, Suppliers, employees, children in conflict with law, parents, guardian, community members</p>	<p>No guidance documents on PI (policies &amp; procedures therefore in violation of P1, P2. No consent for further sharing PI therefore in violation with P4. No Quality controls and constant update of PI therefore in violation with P5. Data subject is notified of on possible sharing PI with 3<sup>rd</sup> party therefore in compliance with P6</p> <p>Most of the documents are store in a non-lockable cabinets, boxes, shelves and unlocked offices. This is compromising the security control measures of ensuring confidentiality, integrity, and security of PI therefore there is no compliance with P7.</p> <p>Processes are in place to allow data subject to update PI therefore in compliance with P8</p>	<ol style="list-style-type: none"> <li>1. Employees should be educated on Security breach procedure after it has been amended to incorporate PI</li> <li>2. Everyone within the supervision of the individual office/branch/programme should be understand the implications of POPIA in her/his process.</li> <li>3. Policy guiding framework should developed to guide the entire Department.</li> <li>4. Further Processing of PI should be accompanied by a standardized Departmental consent statement.</li> <li>5. CFO branch should issue a statement to all their data subjects in relation to POPIA as required in P 5, P6 and P8.</li> <li>6. All data collection/processing tools should be used after a Departmental/National consent statement.</li> <li>7. Data collection tools should have a Departmental disclaimer in relation to PI processing.</li> <li>8. Review of records management and information management policy to include POPIA compliance requirements and measures</li> <li>9. Review of Departmental physical storage facilities and including offices with PI information to be more secured with locks, and lockable storage facilities or digitized.</li> <li>10. Update Corporate risk register to include PI storage</li> </ol>
--------------------	--	--	---	---



Province of the  
**EASTERN CAPE**  
SOCIAL DEVELOPMENT

Beacon Hill Office Park - Corner of Hargreaves Road and Hockley Close - Private Bag X0039 - Bisho - 5605 - REPUBLIC OF SOUTH AFRICA.  
Tel: +27 (0)43 605 5066 - Fax: 043 605 548 Email address: [mncedisi.gazi@ecdsd.gov.za](mailto:mncedisi.gazi@ecdsd.gov.za) Website: [www.socdev.ecprov.gov.za](http://www.socdev.ecprov.gov.za)

Surname, names, ID, address, community ID, telephone no, age, disability, marital status, Employment, Educational details, history, homeowner details, health profile, grant details, feeding scheme details, business ownership details, date of birth, emergency contact, highest grade Means of verification: NISIS profile tool, Data reporting templates tools, NPO cooperative registration, BAS entity forms,

Enumerator /interviewer, community members, household, youth, women, NPO cooperatives, Change agents, shelters, training providers, project participants

No guidance documents on PI (policies & procedures therefore in violation of P1, P2. No consent for further sharing PI therefore in violation with P4. No Quality controls and constant update of PI therefore in violation with P5. Data subject is notified of on possible sharing PI with 3<sup>rd</sup> party therefore in compliance with P6  
Most of the documents are store in a non-lockable cabinets, boxes, shelves and unlocked offices. This is compromising the security control measures of ensuring confidentiality, integrity, and security of PI therefore there is no compliance with P7.  
Processes are in place to allow data subject to update PI therefore in compliance with P8

1. Employees should be educated on Security breach procedure after it has been amended to incorporate PI
2. Everyone within the supervision of the individual office/branch/programme should be understand the implications of POPIA in her/his process.
3. Policy guiding framework should developed to guide the entire Department.
4. Further Processing of PI should be accompanied by a standardized Departmental consent statement.
5. CFO branch should issue a statement to all their data subjects in relation to POPIA as required in P 5, P6 and P8.
6. All data collection/processing tools should be used after a Departmental/National consent statement.
7. Data collection tools should have a Departmental disclaimer in relation to PI processing.
8. Review of records management and information management policy to include POPIA compliance requirements and measures
9. Review of Departmental physical storage facilities and including offices with PI information to be more secured with locks, and lockable storage facilities or digitized
10. Update Corporate risk register to include PI storage.
11. Apply for a prior authorization from Information Regulator for historical PI and SPI
- 12.

ISS branch	Surname, names Residential, postal address; ID number; location information; race, gender, sex; pregnancy, marital status, national, ethnic, age, physical or mental health, well-being, disability status, language, confidential correspondence; education; medical, financial, employment history, income status, HIV /AIDS Status, guardian, parents details, next of kin details	NPOs, Suppliers, employees, children in conflict with law, children, parents, guardian, community members	<p>No guidance documents on PI (policies &amp; procedures therefore in violation of P1, P2. No consent for further sharing PI therefore in violation with P4. No Quality controls and constant update of PI therefore in violation with P5. Data subject is notified of on possible sharing PI with 3<sup>rd</sup> party therefore in compliance with P6</p> <p>Most of the documents are store in a non-lockable cabinets, boxes, shelves and unlocked offices. This is compromising the security control measures of ensuring confidentiality, integrity, and security of PI therefore there is no compliance with P7.</p> <p>Processes are in place to allow data subject to update PI therefore in compliance with P8</p>	<ol style="list-style-type: none"> <li>1. Employees should be educated on Security breach procedure after it has been amended to incorporate PI</li> <li>2. Everyone within the supervision of the individual office/branch/programme should be understand the implications of POPIA in her/his process.</li> <li>3. Policy guiding framework should developed to guide the entire Department.</li> <li>4. Further Processing of PI should be accompanied by a standardized Departmental consent statement.</li> <li>5. CFO branch should issue a statement to all their data subjects in relation to POPIA as required in P 5, P6 and P8.</li> <li>6. All data collection/processing tools should be used after a Departmental/National consent statement.</li> <li>7. Data collection tools should have a Departmental disclaimer in relation to PI processing.</li> <li>8. Review of records management and information management policy to include POPIA compliance requirements and measures</li> <li>9. Review of Departmental physical storage facilities and including offices with PI information to be more secured with locks, and lockable storage facilities or digitized</li> <li>10. Update Corporate risk register to include PI storage</li> <li>11. Apply for a prior authorization from Information Regulator for historical PI and SPI</li> </ol>
------------	---	---	---	--

