

Protection of Personal Information (POPIA) Policy

AREA OF APPLICABILITY

ACROSS AIRPORTS COMPANY SOUTH AFRICA SOC LIMITED AND ITS SUBSIDIARIES

Governance and Assurance

Next Revision Date

05th December 2022

Control Disclosure:

Confidential

Protection of Personal Information (POPIA) Policy
Confidential

Table of Contents

1. Scope	3
2. Objective.....	3
3. Definitions and Abbreviations.....	3
3.1 Definition	3
3.2 Abbreviations.....	5
4. Policy General	5
4.1 Main principles of Conduct.....	5
4.1.1 Eight Conditions of POPIA ACT.....	5
4.1.2 Personal Information Life Cycle	8
4.1.3 Additional rights and obligation not grouped under the 8 POPIA conditions.....	8
4.1.4 Information Officer	8
4.1.5 Training and Awareness	9
4.1.6 General Data Protection Regulation	9
4.2 Key Outcomes of Principals.....	9
5. Process for Monitoring	9
6. Accountabilities and Responsibilities	10
7. Verification.....	10
8. Non-Conformance and Non-Compliance	10
9. Related Policy Document.....	10
10. Related Legislation and Standard	11
11. Change Control.....	11
12. Records	11
13. Revision History.....	11
14. Endorsement (See Master in Policy Management Storage Room).....	12

Protection of Personal Information (POPIA) Policy

Confidential

1. Scope

This policy intent to set out principles in relation to POPIA and is applicable across the organisation to all employees, including the organisation 's subsidiaries, consultants, service providers, stakeholders, members of the Board and concessions where the exchange of personal information is warranted. The policy also applies to the processing of personal information entered in a record by making use of automated or non-automated means.

2. Objective

To provide guidance on how the Organisation must comply with the obligations created by the Protection of Personal Information Act 4 of 2013.

To set out POPIA conditions and other POPIA compliance requirements and clarify key responsibilities and obligations of the various role players in Airport Company South Africa SOC Limited

3. Definitions and Abbreviations

3.1 Definition

ACT

Protection of Personal Information Act 4 of 2013.

Conditions

Conditions of Lawful Processing stipulated in Chapter 3 of the Act.

Constitution

Constitution of the Republic of South Africa 1996.

Data Subject

Means the person to whom the personal information relates. This includes customers, employees, suppliers, contractors, vendors, third parties and stakeholders.

De-identification

Is the process used to prevent a person's identity from being connected with information.

Employee

An officially appointed person to Airports Company South Africa SOC Limited., irrespective of the duration or nature of their appointment - permanent or temporary.

Protection of Personal Information (POPIA) Policy

Confidential

Information Officer

The designated employee within the organisation responsible to ensure that the Organisation complies with POPI Act; the role is prescribed in the Act.

Information Regulator

The Information Regulator (South Africa) is an independent body established in terms of section 39 of the Protection of Personal Information Act 4 of 2013. The Information Regulator is responsible for protecting data subjects against harm and to ensure that their personal information is protected by responsible parties.

Organisation

Airports Company South Africa SOC limited.

Operator

means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

Process

means any operational activity concerning personal information including the collection, organisation, storage, modification, communication and destruction of information.

POPIA

Protection of Personal Information Act 4 of 2013.

Personal Information

Means information relating to the identifiable, living, natural person and where it is applicable, and identifiable juristic person, including but not limited to –

- information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic, or social conscience, belief, culture, language and birth of a person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other assignment to the person;
- the biometric information of a person;

Protection of Personal Information (POPIA) Policy

Confidential

- the personal opinions, views or preferences of the person;
- the views or opinions of another individual about the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; and
- the name of the person if it appears with other personal information relating thereto.

Record

means any recorded information in whatever form in possession or under the control of Airports Company South Africa SOC Limited.

3.2 Abbreviations

Abbreviation	Description
POPIA	Protection of Personal Information Act
PAIA	Promotion of Access to Information Act
PI	Personal Information
GDPR	General Data Protection Regulation
IO	Information Officer

4. Policy General

The right of privacy is enshrined in the South African Constitution which expressly states that everyone has the right to privacy. The POPI Act is aimed at facilitating the protection of this important right.

This policy establishes measures and standards for the protection and lawful processing of personal information within the organisation and provides principles regarding the right of individuals to privacy and to reasonable safeguarding of their personal information.

The organisation shall comply with both the law and good practice, respect individuals' rights to privacy, be open and honest with individuals whose data is held, provide training and support for staff who handle personal data, so that they can act confidently and consistently protect personal information and keeping information securely.

4.1 Main principles of Conduct

4.1.1 Eight Conditions of POPIA ACT

POPIA places a responsibility on the organisation to promote the lawful processing of personal Information and its service providers who act on behalf of the organisation.

UNCONTROLLED COPY WHEN PRINTED

Protection of Personal Information (POPIA) Policy

Confidential

POPIA consist of eight conditions which are adopted by the organisation as principles guiding the organisation to comply with the obligations created by the POPIA. The conditions are as follows:

- **Condition 1 – Accountability**

The Organisation is accountable and responsible for personal information in its possession at an organisational level and shall comply with all the 8 POPIA conditions, including its operators and subsidiaries.

Divisions and Departments are accountable and responsible for personal information they process in their respective business units. Each employee is responsible to comply with POPIA, POPIA Policy and POPIA Procedure as they process personal information in their different Divisions.

- **Condition 2 - Processing Limitation**

The Organisation shall ensure that the processing of any personal Information is done in accordance with the relevant legislation without infringing on the data subjects right to privacy.

The Organisation shall ensure that personal Information is only processed if the reasons given for the processing are adequate, legitimate, relevant and not excessive. Personal information shall be processed for the purpose it was collected for and not for a different purpose unless in accordance with exceptions in the Act.

- **Condition 3 - Specific Purpose**

The organisation shall only collect personal Information for a specific purpose which is explicitly and limit the processing to the specific purpose it was collected for. The Organisation must ensure, in collecting the information, that the data subject is aware of the purpose for which the information is being collected.

- **Condition 4 - Further Processing Limitation**

The further processing of any personal information must be compatible with the purpose for which it was initially collected for.

- **Condition 5 - Information Quality**

The Organisation shall take reasonable steps to ensure that the personal Information it processes, and stores is complete, accurate, not misleading and kept up to date where necessary.

Protection of Personal Information (POPIA) Policy

Confidential

- **Condition 6 - Openness**

The Organisation must maintain the documentation of all processing operations under its responsibility. The purpose of this condition is to ensure transparency and fairness in the processing of personal information.

The Organisation shall ensure that the data subject is aware of the reasons for which his/her personal Information is processed. The Organisation shall inform data subjects of any breaches relating to the Data Subject personal information.

- **Condition 7 - Security Safeguards**

The organisation shall secure the integrity and confidentiality of personal information in its possession through the implementation of appropriate measures to prevent; the loss, damage and unauthorised destruction of personal Information; and unlawful access which leads to processing of personal Information without the consent of the data subject.

IT will guide the organisation in terms of what are the appropriate IT security technologies to ensure safeguarding and protection of automated personal information and educate employees on protecting and securing automated processing of personal information.

Security Enterprise and Infrastructure Asset Management will guide the organisation in terms of appropriate security measures and facilities to ensure safeguarding and protection of non-automated personal information.

The Organisation shall also ensure that it has written agreements with all Operators processing personal Information on its behalf. These agreements will need to outline the Operators measures to ensure the protection of personal Information in their possession.

The Organisation shall establish and implement processes or mechanisms to notify a data subject and the Information Regulator where there are reasonable grounds to believe that the personal Information of a data subject has been accessed or acquired by any unauthorised person.

- **Condition 8 - Data Subject Participation**

The Organisation shall establish mechanisms and processes to provide data subjects with the opportunity to request, correct, delete or destroy their personal information insofar as requests have been done in the prescribed manner and where possible and justifiable.

Protection of Personal Information (POPIA) Policy

Confidential

4.1.2 Personal Information Life Cycle

Processing includes any activity concerning personal information. When employees, operators or the Organisation Subsidiaries:

- Collects Personal Information;
- Use Personal Information;
- Share Personal Information;
- Transfer Personal Information;
- Store Personal Information; and
- Destroy Personal Information;

shall do so in accordance with compliance requirements of POPIA Act, Protection of Personal Information (POPIA) Policy – I010 002P and [Protection of Personal Information \(POPIA\) Procedure - I010 002M](#).

4.1.3 Additional rights and obligation not grouped under the 8 POPIA conditions:

- Processing of special personal information;
- Processing of Children’s personal information;
- Direct Marketing;
- Processing subject to prior authorisation;
- Profiling of data subjects based on the automated processing of PI;
- Transfer of PI to other countries;
- Notification to the Regulator;
- Assessments;
- Information Notices;
- Enforcement Notices and Administrative fines.

The organisation shall take proper measures and controls to ensure compliance with these obligations. The [Protection of Personal Information \(POPIA\) Procedure - I010 002M](#) will provide guidance in terms of how to implement these additional obligations.

4.1.4 Information Officer

The Organisation shall appoint an Information Officer in terms of section 55 of the Act. The Information Officer after the effective date has been announced may only take up her/his duties in terms of the Act after the Organisation has registered him /her with the Information Regulator.

Protection of Personal Information (POPIA) Policy
Confidential

4.1.5 Training and Awareness

Heads of Divisions shall ensure that all their staff members are trained on how to process personal information in accordance with the Act. The information Officer shall be responsible to provide such training and general awareness. Head of Divisions shall appoint POPIA Champions to assist with implementation of POPIA in the respective divisions.

4.1.6 General Data Protection Regulation

The Organisation must determine, based on its business model, if the Organisation activities falls within the ambit of the GDPR. Based on the assessment if the GDPR applies to the Organisation, shall identify such activities, its risks and develop and monitor controls to minimise the risks associated with breach of GDPR.

4.2 Key Outcomes of Principals

- Organisational Compliance with the POPIA Act.
- Protection of personal information within the organisation.
- Promotion of a privacy culture.
- A cross functional coordinating POPIA Champions
- Enhanced personal information security safeguards.

5. Process for Monitoring

The effective implementation and monitoring of this Protection of Personal Information (POPIA) Policy shall be done through relevant committees. Internal audits shall be conducted accordingly to determine conformance and implementation. This policy shall be reviewed accordingly to reflect the environmental changes or regulation requirement in order to ensure that is relevant and current to the organisation.

MONITORING CONTROLS	PURPOSE	RESPONSIBLE	FREQUENCY
Internal Audit	Provide the Board, Executive and Audit committee an independent oversight with regards to conformance to this procedure.	Chief audit Executive	Planned Intervals

Protection of Personal Information (POPIA) Policy
Confidential

Note: This policy shall be reviewed in three-years cycle and if there is a need to review the policy before three-years cycle lapses due to any circumstances being legal requirements, changes in the businesses, the need to reflect current practices or activities, the policy shall be unlocked for review accordingly.

6. Accountabilities and Responsibilities

The overall accountability for development and implementation of this procedure lies with the Chief Executive Officer with the support from Group Executive: Governance & Assurance and Information and Privacy Specialist as the responsible persons for actual development, implementation of this procedure. Internal Auditors have full responsibility to report audit outcomes to Audit committee about the affairs of legal department.

RESPONSIBLE	ACCOUNTABLE	CONSULTANT	INFORMED
Group Executive: Governance and Assurance	Chief Executive Officer	Specialist: Information and Privacy	Employees & Managers
Has overall responsibility for actual, development, implementation and adherence of this policy	Has overall accountability for development and implementation of this policy	Consulted at the time of an exception and adherence of this policy.	Has overall responsibility for adherence, implementation and performance of a given task.

7. Verification

This policy shall be verified in accordance with [Verification Policy Document - Z001 002M.](#)

8. Non-Conformance Reporting

Any deviation from this policy shall be identified and registered with corrective and preventative measures for continual improvement in accordance with [Non-Conformance Policy Document - Z001 001M.](#)

9. Related Policy Document

- Document Control Procedure - Z001 006M
- Record Keeping Requirements Procedure - Z001 008M
- Code of Ethics - J060MAN
- Employee Manual - H0100MAN
- Anti-Corruption Management Plan as Amended
- Supply Chain Management Procedures Manual (Latest Version)
- Gift Policy - J060 001P
- Board Members of Third Party Companies Policy - J030 003P

UNCONTROLLED COPY WHEN PRINTED

Protection of Personal Information (POPIA) Policy
Confidential

Protection of Personal Information (POPIA) Procedure - I010 002M

10. Related Legislation and Standard

Promotion of Access to Information Act No. 2 of 2000
Protection of Personal information Act No. 4 of 2013
Quality Management System ISO 9001

11. Change Control

This policy shall only be changed with the authorisation of the Chief Executive Officer and in accordance with [Change Control Policy Document - Z001 003M](#).

12. Records

Record Name	Storage Location	Record Number	Responsible Person	Retention Time
Protection of Personal Information (POPIA) Policy	Master in Policy Management Storage Room	I010 002P	Policy Assurance Officer	Three (3) years
Protection of Personal Information (POPIA) Procedure	Master in Policy Management Storage Room	I010 002M	Policy Assurance Officer	Three (3) years

13. Revision History

Date last revised	Revision Status	Compiler	Summary of changes
New Document	Issue: 1	Specialist: Information and Privacy NAME AND SURNAME Sherly Mphahlele	First Issue

Protection of Personal Information (POPIA) Policy
Confidential

14. Endorsement (See Master in Policy Management Storage Room)