AF Access Retirement Fund: Pension Section & Provident Section Privacy Policy

Implemented: 1 July 2021
Reviewed: November 2022
Reviewed and signed: August 2024

Table of Contents

Annexures

1. Introduction

As registered South African private entities the AF Access Retirement Fund: Pension Section and AF Access Retirement Fund: Provident Section ("the Fund") are required to comply with the Protection of Personal Information Act 4 of 2013 (POPIA). The purpose of this POPIA is to give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at balancing the right to privacy against other rights, particularly the right of access to information.

The Fund is committed to the protection and confidentiality of all Personal Information ("PI") for which it is responsible. To assist the Fund to do so, and as is required in terms of POPIA, the Fund has appointed an Information Officer ("IO") and agreed to the duties and responsibilities of the IO as set out in the "Duties and Responsibilities of the Information Officer" document. This is a separate document and it should be referred to as necessary. For ease of reference, this document is included as Annexure B.

The Fund acknowledges that it is a Responsible Party in terms of POPIA. However, it makes use of Operators (service providers) in order to process its PI. The Fund will ensure that written contracts between the Fund and its appointed Operator/s are affected and specifically:

- Authorise the processing of PI,
- Require that all PI which comes to the knowledge of the Operator is treated as confidential and shall not be disclosed unless required by law or in the course of the proper performance of its duties and responsibilities,
- Require that the Operator establish and maintain security safeguards as envisaged in Section 19 of POPIA,
- Require the Operator to immediately notify the Fund where there are reasonable grounds to believe that PI has been accessed or acquired by any unauthorised person,
- Require the Operator to assist the Fund in meeting its obligations in terms of POPIA.

The Fund will establish measures to adhere to any codes of conduct or industry regulations that are applicable. In the event of any conflict, any retirement fund code of conduct recognised by law and applicable to retirement funds and their service providers will take precedence over this Policy.

The Fund recognises that confidentiality and data protection is an infinite journey and there is no absolute compliance destination. The Fund will continually strive for continuous compliance. Striving for compliance aligns to the principles of Treating Customers Fairly ("TCF") and will be embedded in the culture of the Fund in the same way as TCF.

To this end, whilst not a POPIA requirement, it is widely recognised that privacy "by design and by default" is leading international practice and the Fund will require that any new initiatives, activities or products consider data protection and confidentiality requirements during the assessment phase of such activities to ensure that any mandatory compliance requirements, security or controls, or other measures to reduce risk to PI are implemented.

2. Purpose and applicability of the privacy policy

The purpose of this Privacy Policy ("this Policy") is to establish a compliance framework to govern the information handling practices for all PI that is collected or otherwise processed by, or on behalf of, the Fund to achieve its objectives.

Appropriate governance, management and oversight activities will be established to ensure that suitable measures, controls and standards are implemented to enable confidentiality and data protection.

This Policy aims to uphold the rights of Data Subjects, comply with applicable data protection laws and align to international best practice standards.

While this Policy is largely aligned to the requirements of POPIA, international best practices have also been considered. In the event of any ambiguity in interpretation, POPIA will take precedence over any other source.

The Board and officers of the Fund agree to be bound by this Policy, and as applicable, it extends to any service providers, contractors or third parties involved in the processing of PI on behalf of the Fund.

3. Policy statements: Conditions for the lawful processing of PI

The Fund, as a Responsible Party, is accountable for ensuring that the conditions for lawful processing and the measures implemented to give effect to these conditions are complied with, at the time of determining the purpose and means of processing, and during the processing itself. Certain measures have been included in this Policy.

This Policy aligns to the headings and follows the same order that the conditions are listed in POPIA:

a) ''Accountability'', as referred to in section 8;

b) ''Processing limitation'', as referred to in sections 9 to 12;

c) ''Purpose specification'', as referred to in sections 13 and 14;

d) ''Further processing limitation'', as referred to in section 15;

e) ''Information quality'', as referred to in section 16;

f) ''Openness'', as referred to in sections 17 and 18;

g) ''Security safeguards'', as referred to in sections 19 to 22; and

h) ''Data subject participation'', as referred to in sections 23 to 25.

3.1 Processing Limitation

The Fund is established and registered as a "pension fund organisation" in terms of the Pension Funds Act 24 of 1956, as amended ("the Act") with the specific object of providing benefits to members at retirement or to make payments to beneficiaries in the event of death.

In terms of section 13A of the Act, the Fund is obligated to receive payment of contributions and schedules detailing PI of the members of the Fund from employers that participate in the Fund.

Participating employers are obligated in terms of the Act and the Income Tax Act 58 of 1962, as amended, ("ITA") to ensure that eligible employees, as defined in the registered rules of the Fund, are entered as Fund members as a condition of their employment. Participating employers are required to advise the Fund when the service of an employee is terminated, irrespective of the reason for such termination. Accordingly, the employer is a primary source of information related to new entrants, exits and deaths. For this reason, the employer/s is regarded as a "co-Responsible Party" in respect of the processing of PI of Fund members. The Fund and its participating employer/s will therefore agree when and how Personal Information is to be provided by the employer/s directly to Operators or service providers appointed by the Fund and by the Fund to Operators or service providers where mandated to do so by the employer/s.

Following from the above, the Fund records that it collects and processes PI:

1. In compliance with obligations imposed by law,
2. To protect the legitimate interests of Data Subjects as Fund members, and
3. As is necessary to pursue the legitimate interests of the Fund in meeting its objectives.

The Fund is committed to doing so in a reasonable way and that does not infringe on the privacy rights of Fund members. The Fund is further committed to:

a. Uphold, as far as is reasonably possible, the principle of minimality – where only adequate, relevant, and necessary data and/or information, that is not excessive, is collected and processed to achieve the purpose.
b. Develop and communicate processes, including using the forms developed for this purpose by the Information Regulator (IR), to enable Data Subjects to:'

   – Object, where reasonable and lawful, to the collection and processing of their PI,
   – Request that their PI be updated or corrected, and
   – Request and facilitate, where legally feasible, the deletion of PI or restrict processing and access to the PI.

3.2 Purpose Specification

The Fund will establish measures to:

a. Ensure PI is only used for the purpose/s for which it is collected.
b. Notify Data Subjects of the purposes for which the Fund collects and processes their PI, both at the point of collection and during their Fund membership journey. By way of example, the Fund has developed a Privacy Statement that is made available to all new entrants, is included in the member booklet issued to all Fund members, in newsletters issued by the Fund from time to time and in the Fund's annual report.

The Fund is required, in terms of Section 14 (1) of POPIA, to ensure that PI is not retained any longer than is necessary to achieve the purpose for which the information was collected and processed or as otherwise permitted in law, or by way of contractual agreement (and other exceptions listed in Section 14). In addition to PI, the Fund has developed and maintains its own public and internal documents and records.

Section 14(5) of POPIA requires that PI under the Fund's control be destroyed or deleted in a manner that prevents its reconstruction in an intelligible form. Whilst POPIA has placed this obligation on the Fund, it does not prescribe or provide any guidelines on how PI should be deleted or destroyed.

The Board has, therefore, developed this programme to confirm the Fund's documents and records lifecycle, and more specifically its storage, retention and deletion register. This register references the records listed in the manual prepared in terms of the Promotion of Access to Information Act, No 2 of 2000 ("PAIA") and this manual should be consulted as necessary.

The Fund has contracted with a number of Operators (third party service providers), including a licensed administrator, based on their skills and ability to render specified services to the Fund. This programme recognises that these Operators maintain appropriate record management policies. Therefore, this programme will not in any way impact these record management policies, with the exception of the storage, retention and deletion register attached as Annexure C to this Policy. As necessary, relevant Operators will be instructed to, as a minimum, comply with the content of the register.

This programme recognises that the Board and officers of the Fund are accountable for and required to adhere to the principles established in respect of confidential information and PI within their control. The Board has committed, in terms of its Code of Conduct to protect and safeguard confidential information and PI and to adhere to the contents of this programme in relation to the storage, retention, deletion/ destruction measures adopted.

In terms of this programme:

1. Format of documents and records

It is recognised that documents and records can either be in electronic or physical format:

Physical - original paper copies, printouts or any format which can be read without the use of a computer device.

Electronic – recorded in a manner that requires a computer or electronic device to display, interpret and process.

This programme applies to physical and electronic records, including but not limited to:

- typed, or printed hardcopy paper documents;
- electronic records and documents (for example, email, Web files, text files, PDF files);
- video or digital images;
- graphic representations;
- electronically stored information contained on network servers and/or documents;
- management systems; and
- recorded audio material (for example, voicemail, voice recordings).

2. Classification of documents and records

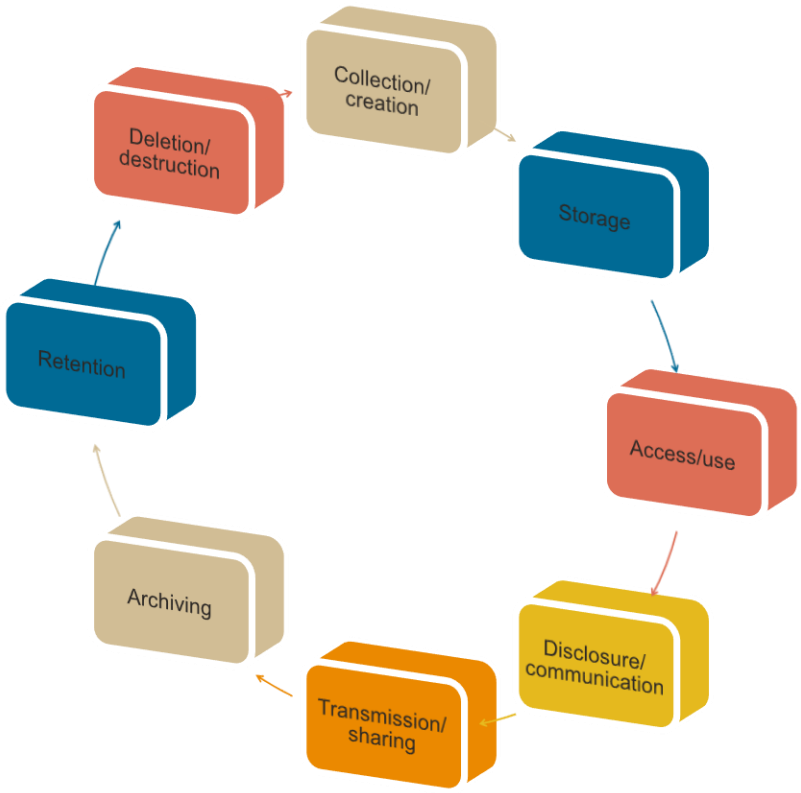
Documents and records are classified to determine the storage and retention security safeguards to be applied - as required in terms of Section 19 of the Act (requires the Fund to secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information).

The classification to apply is detailed below, with the exception of public documents/records, this list of examples is not exhaustive:

Classification level	Examples	Guidance
Public	• Registered rules • Audited annual financial statements • PAIA Manual	Required to be submitted to the Financial Sector Conduct Authority (FSCA) and in consequence is available to the general public. Submitted to the IR and in consequence is open for inspection.
Internal	• Agendas for, and minutes of, Board and Sub-Committee meetings held • Governance policies, procedures, practice notes, and registers • Communication to stakeholders • Correspondence with stakeholders, the FSCA or any regulatory body • Contracts with service providers • Documents related to litigation matters	All internal documents and records are confidential. Access to confidential information could pose a high risk to the Fund from a regulatory perspective, but only a moderate risk from an operations perspective. As such, reasonable security safeguards are to be employed in the storage and retention of internal information.
Confidential	Personal Information as defined in POPIA.	Access to confidential information could pose a high risk to the Fund from a regulatory perspective, but only a moderate risk from an operations perspective. Reasonable security safeguards are to be employed in the storage and retention of confidential information. All Personal Information is confidential.
Sensitive	Special Personal Information as defined in POPIA (for example, health data, race, religion, banking details, etc.)	Sensitive documents and records, if disclosed, destroyed, or altered inappropriately could pose a significant risk to the Fund from a regulatory or operations perspective. Far more rigorous security safeguards must be applied in the storage and retention of sensitive information. All Special Personal Information is sensitive.

3. Lifecycle of documents and records

The lifecycle extends to the collection, creation, processing, storage, access, use, disclosure (or communication, transmission, sharing, retention, archiving, deletion and destruction of documents and records.



4. Principles regarding the lifecycle of documents and records

The Board and Fund officers will implement the following regarding documents and records:

- When requested from Operators, must contain the minimum amount of content necessary to enable the legitimate processing required, or to allow a decision to be taken,
- May only be used for the purpose intended and that which is not used will not be retained or stored and must be returned to the IO for deletion and destruction, or deleted/destroyed as instructed by the IO,
- Must always be safely secured and stored in such a way as to maintain the integrity of the content,
- May not be shared, communicated or transmitted, unless authorised, in writing, by the Board,
- Only the “final” draft will be stored and retained, and
- Will not be duplicated or retained indefinitely, unless authorised by the IO.

5. When a Board member and/or Fund officer leaves office:

- All paper documents and records must be returned to the IO for deletion and destruction. The IO will determine the recycling approach, if any, to apply.
- Electronic documents and data retained on computers and devices must be appropriately deleted to ensure that content cannot be reconstructed in intelligible form and a contractual undertaking in this regard will be required.
- The departing Board member or Fund Officer must complete and submit a statement to the IO confirming that the fund specific electronic documents and data on their computers and devices (including backup) has been deleted.

6. Data storage, retention, deletion and/or destruction

The Board and Fund officers direct that the documents and records listed in Annexure C:

- Must be stored in accordance with the security and safeguarding classification indicated. A contractual undertaking in this regard will be required,
- Must be retained for at least the minimum period indicated,
- Must be deleted and/or destroyed as stipulated and in accordance with the provisions of clause 5 above, provided that the IO may agree with a relevant Operator that the Operator will delete and/or destroy the documents and/or records. A contractual undertaking in this regard will be required.

3.3 Further Processing

The Fund will adopt measures to ensure that any additional processing of PI by the Fund is compatible with the original purpose/s for which it was collected. The Fund will contract with its service providers to require that any additional processing of PI is compatible with the original purpose/s for which it was collected.

The Fund considers the following processing to be compatible with the original purpose/s:

a. In compliance with the FSCA's "fit and proper" requirements/assessments applicable to Trustees.
b. In compliance with applicable laws, including the ITA, provided that suitable security safeguards are in place.
c. For the conduct of any proceedings in court, the Adjudicator or a tribunal.
b. Where PI has been de-identified and cannot be linked back to a Data Subject.

3.4 Information Quality

The Fund will adopt measures to ensure that PI processed is updated to be accurate, complete and not misleading. As necessary, the Fund will:

1. Engage with the Participating Employers, as the primary sources of information, to assist in ensuring that PI processed is updated to be accurate, complete, and not misleading, and
2. Contract with its service providers to require that processes be established so that PI processed is updated to be accurate, complete and not misleading. This may include making mechanisms available to Data Subjects to access and update their own information.

3.5 Openness

The Fund will include in its Communication Policy and plan, communication to specifically notify Fund members of their rights in terms of POPIA, that they are able to lodge a complaint or request for details of their PI held by the Fund with the IR and the contact details of the IR.

As the Fund contracts with a number of third parties, the Fund will include in its communication to Fund members a list of third parties who have access to Fund member PI and the reasons for such access.

Where the Fund, as Responsible Party, is implicated in a complaint, the following will apply:

a) The IO will circulate, for information purposes, a copy of the complaint to the Board within 5 working days of receipt of the notification from the IR,
b) The IO will engage with the office of the IR as set out in the "Roles and responsibilities of Information Officer" document,
c) As necessary, the IO will request the Board's assistance in the complaint resolution process, and
d) Where it is necessary to engage experts and/or service providers to assist in the complaints resolution process, obtain engagement authorisation from the Board in accordance with agreed procurement and expense policies applicable.

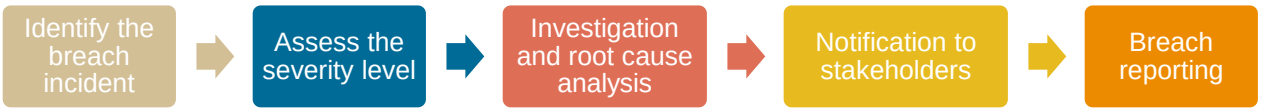
The IO is required to complete the Complaints Register attached as Annexure D, include the register at each formal meeting as indicated by the Board, and report to the Board on recommendations in improving processes, measures, controls and standards applicable to minimise/better manage a reoccurrence of the complaint.

3.6 Security Safeguards and Breach Management Protocols

Where the Fund becomes aware of, or where there are reasonable grounds to believe that sensitive or confidential information has been unlawfully accessed, or processed, or acquired by an unauthorised person ("an information breach" or "security compromise"), the Fund is required to notify the IR and the Data Subjects affected:

1. As soon as reasonably possible after the compromise, and
2. Such notification must include the following:
    - information about the compromise (as much detail as possible about the how and what),
    - the consequences and dangers of the compromise,
    - the measures taken/to be taken to remediate the compromise,
    - recommendations on what the Data Subjects can do to protect themselves, and
    - the identity of the perpetrator (if known).

To comply, with its reporting requirements to the IR, its obligations to notify Data Subjects and to develop management/mitigation strategies, the Fund will follow the process below should an information breach occur:



Identifying the breach incident

An information breach might occur in several ways, such as:

- Email sent to incorrect third party.
- Loss of papers containing sensitive or confidential information.
- Loss of electronic device (for example, a phone or laptop) containing sensitive or confidential information.
- A cyber-attack (a hack) on systems containing PI or Fund data.
- Unauthorised sharing of information by a third party or a cyber-attack on a third party who has received or has control over PI or Fund data.

Assessing the severity of the breach

The assessment criteria to be used will depend on the cause and consequences of the compromise.

The following criteria should assist in determining the severity and impact of the compromise, this list is not exhaustive:

1. The number of Data Subjects impacted,
2. The content of the sensitive or confidential information/data compromised, for example ID number, bank account details, personal health information, child information, etc, to assess how this could be used to prejudice the Data Subject,
3. Likely prejudice or impact to the Data Subjects, including the Fund,
4. Likely financial loss that the Fund could be exposed to, including any fines that may be imposed
5. Reputational damage to Fund.

The IO will assign the following severity level based on his/her assessment criteria, with the assessment indicated being an illustration:

Severity Rating	Assessment
Marginal	Very few Data Subjects involved, data compromised minimal and does not include Sensitive Personal Information or child information, no risk of loss to Fund and Data Subjects
Limited	More Data Subjects involved, more data compromised but does not include Sensitive Personal Information or child information, low risk of loss to Fund and Data Subjects

Severe	More data compromised or includes Special PI/child information. Medium risk of loss to Fund and/or prejudice to Data Subjects but no reputational risk to Fund
Catastrophic	Many data subjects involved; extensive data breach includes Special PI/child information. High risk of loss to Fund and/or prejudice to Data Subjects and reputational risk

Investigating the breach

When the IO has been advised of an actual compromise or where there is reason to believe a compromise has occurred, the IO will respond at the earliest opportunity by identifying the breach incident/likely breach incident, investigating the root cause of the compromise and determining:

1. The severity of the breach,
2. The various remediation measures available,
3. The most appropriate remediation response given the nature of the compromise,
4. The potential costs of remediation and communication,
5. What measures Data Subjects could take to protect themselves and, as applicable, how the Fund would be able to assist,
6. Whether any external professional expertise is required to investigate, manage and resolve the compromise.

The IO will prepare a report detailing the outcome of the investigation, the root cause, the severity assessment and his/her recommendations regarding appropriate management, remediation and resolution measures for the Board to consider. This report must remind the Board of the notification requirements.

On receipt of the report, the Chairperson will advise the Communication Sub-Committee to initiate the communication response to stakeholders including the IR. The Chairperson is to ensure that the Communication Sub-Committee understands that:

- This notification must be made as soon as reasonably possible after the discovery of the compromise, in line with the Fund's crisis communication plan, and considering the legitimate needs of law enforcement.
- The Fund will need to delay notification to Data Subjects and other stakeholders, excluding the IR, if a public body responsible for the prevention, detection or investigation of offences or the IR determines that notification will impede a criminal investigation by the public body concerned.
- The IR may direct the Fund to publicise, in any manner specified, the facts of any compromise to the integrity or confidentiality of PI in circumstances where the IR has reasonable grounds to believe that such publicity would protect a Data Subject who may be affected by the compromise.

Breach reporting

The IO will complete the breach register following every compromise investigation and report issued.

The Fund's breach register is attached as Annexure E.

3.7 Data Subject Participation

Access to, and correction or updating of PI

The Fund has developed a manual in terms of Sections 14 and 51 of PAIA. The IO will assist the Board in maintaining and updating the manual to include POPIA provisions and to maintain this manual. This is a separate document and should be referred to as necessary.

The Fund will establish appropriate channels and mechanisms so that Data Subjects can access and correct or update their PI, or exercise any rights that they have under POPIA, provided that:

- An individual's identity must be suitably established before granting access to PI related to them.
- If a third party wishes to gain access to PI, they must provide the consent of that Data Subject, a court order, or otherwise have a legitimate and lawful requirement for obtaining such information.

The Fund reserves the right to reject requests that do not adhere to these requirements and/or refuse requests as provided for in Chapter 4 Part 2 and Chapter 4 Part 3 of PAIA.
As necessary, the Fund will:

1. Engage with the Participating Employer/s, as the primary source of information, to assist Data Subjects with requests to correct or update their PI, and
2. Contract with its service providers to require that processes be established to assist Data Subjects with requests to:
   (a) access PI that is related to them and readily accessible or where the Data Subject has provided consent to a third party granting such access (for example where a financial adviser is given consent to access his/her client's information).
   (b) correct or update their PI. This may include making mechanisms available to Data Subjects to access and update their own information.

It is specifically recorded that all requests for PI in terms of a court order or as enabled by PAIA, and detailed in the PAIA Manual, are to be directed to the IO. The IO is tasked with the necessary oversight in arranging access to the information or directly responding where access is refused. The IO will on a quarterly basis report to the Board on requests received by completing the register indicating the request, reasons for request and response provided. The register is attached as Annexure F.

Requests objecting to processing or for deletion of PI

All requests objecting to the processing of PI or for the deletion of PI must be completed using the Forms indicated below and directed to the IO to attend to:

1. A Data Subject who wishes to **object** to the processing of Personal Information must submit the objection using Form 1 attached as Annexure G.
2. A data Subject who wishes to request the **deletion** of Personal Information must submit the request using Form 2 attached as Annexure H.

The IO will assist, free of charge, the Data Subject in completing requests and responding to such requests.

The IO will on a quarterly basis report to the Board on requests received by completing the registers indicating the requests received, reasons for the request and the response to the Data Subject. These registers are attached as Annexure I and Annexure J respectively.

3.8 Special Personal Information

Whenever categories of Special Personal Information (for example, race, medical / health data, children's information, etc.) are processed, the Fund will apply more stringent security controls, particularly if disclosure or unauthorised access to this data may cause damage or distress to a Data Subject.

Further:

a. As far as possible and practical, the Fund will keep records of access to all special personal information.
b. If collection of special personal information is mandated by law (for example, in the disposition of death benefits in terms of section 37C of the Act), consent does not need to be obtained, but for any other purposes related to special personal information, the Fund will collect and maintain records of explicit consent in this regard.

3.9 Direct Marketing

The Fund and Alexforbes may partner to provide information to employers and members about services and products offered by the Alexforbes Group linked to the financial well-being of participating employers and members. Any intentions to do so not directly related to the responsibilities of the fund as required by the Pension Funds Act will be considered and managed by the Fund, with the necessary consent from Data Subjects being sought prior to implementation.

3.10 Automated Decision Making

The Fund does not engage in any automated decision making, algorithms or profiling which may have a significant impact on a Data Subject, with the exception of those provided for by law (for example, underwriting by an insurer for insured benefit purposes, risk profiling by an insurer to set a premium rate, etc.). The Fund will therefore not subject any Data Subject to a decision based purely on automated decision making.

3.11 Transborder Information Flows

The Fund adheres to the requirements stipulated in POPIA for the transmission of PI across international borders, where this is a requirement. This section specifically requires that any personal information about a data subject provided to a third party may not be transferred outside of South Africa, unless the third party is subject to substantially similar privacy laws as in the RSA. In the event of the distribution of death benefits to beneficiaries and third parties representing minor beneficiaries who may not reside in South Africa, such information flow is allowed given that the processing of their personal information was for their benefit,

3.12 Regulatory Authorisation

The Fund does not perform any activities that require prior authorisation from the IR. The Fund's IO will monitor the Fund's operations and request such authorisation from the IR should it be required.

3.13 Personal Information Impact Assessment

The IO of the Fund is required to ensure that a Personal Information Impact Assessment (PIIA) is undertaken by the Fund, the purpose being to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of PI.

The IR has not provided detailed guidelines on performing PIIAs, nonetheless, the Fund understands that it must consider the impact that its information processing activities will have on PI in general, and the risks to such information. Accordingly, the Fund has developed a PIIA framework that will allow an initial assessment of its compliance, and thereafter, as its understanding of the data protection and privacy environment grows, will also enable a more rigorous assessment of risk.

Objective

The Fund has prepared a PIIA to identify where the Fund risks non-compliance with the conditions for lawful processing and the high risk processing activities that the Fund engages in, especially those which may negatively impact the rights of Data Subjects. The Fund will use the outcome of its PIIA to implement suitable controls to minimise the areas of risk as far as reasonably possible.

Frequency

The Fund will review its PIIA as necessary, but at least annually, or in response to any changes to regulations, in line with any guidelines issued, and other changes, for example, to the Fund's information processing operations, service providers, technology, market changes which may affect the Fund, etc.

PIIA Process

1. Identify risks

The Fund will:

a. Determine the categories of risk it wishes to evaluate itself against, at a minimum to include the conditions for lawful processing of PI to established a baseline level of compliance, but, may add others as appropriate to the specific needs of the Fund or its information processing practices.
b. In time, the Fund may follow a more rigorous approach by assessing risk at a deeper level by completing the Personal Information Inventory and assessing risk per record of PI. At a minimum, the Inventory is aligned to the records listed in the Fund's PAIA Manual.

2. Evaluate risks

The Fund will:

a. For each of the risks identified in the first step, determine the level of risk (risk rating) per item.
b. This is done by considering the likelihood that a risk will occur, as well as the impact (or likely harm) that it will have on the Fund or on the PI processed by the Fund.
c. A risk matrix is then used to determine the risk rating.

Risk Matrix					
Impact on the fund	Likelihood of occurrence				
		Highly unlikely	Unlikely	Likely	Highly Likely
		1	2	3	4
Marginal	1	1	2	3	4
Limited	2	2	4	6	8
Severe	3	3	6	9	12
Catastrophic	4	4	8	12	16

In this way, the Fund will have an indication of the areas on which it needs to focus its immediate attention. In this context, a risk is an indicator of where something could go wrong, not necessarily where an incident has already occurred.

3. Treat risks

The Fund will prioritise and address risks according to the following guidelines:

Risk Rating	Action
Critical	• Start corrective action immediately, to be addressed within the next 3 months. • Monitor closely to verify success. • Consider stopping the activity where appropriate/ practical to do so.
High	• Start corrective action within the next 3 months, to be resolved within the next 6 months. • Monitor to verify success.
Moderate	• Take action in line with operational requirements, or review action to be taken within 6-months.
Low	• Housekeeping activity / low risk. Low priority for action.

The Fund will periodically monitor and review all risks, even the low rated ones, to ensure that if any changes impact the Fund, they do not also change the identified risk ratings.

The PIIA framework is attached to this Policy as Annexure K.

4. Fund governance framework and policies

The Fund has an established broader governance environment and maintains specific policies to record the principles of good governance that are aspired to and applied in respect of, and on behalf of, the Fund. The Board will review all other governance policies to assess whether any amendments are required to either ensure compliance with POPIA or record its aspirational principles in its compliance journey.

5. Adoption

This Policy is hereby adopted by the Board of Trustees of the AF Access Retirement Fund: Pension Section and Provident Section:

Signed by:HERBERT ROBIN HURD Signed at:2024-08-12 13:13:02 +02:00 Reason:Witnessing HERBERT ROBIN H	Signed by:Nomonde Zwane Signed at:2024-08-16 11:26:52 +02:00 Reason:Witnessing Nomonde Zwane	Signed by:Michael Frederick Prinsloo Signed at:2024-08-16 12:22:21 +02:00 Reason:Witnessing Michael Frederick Pri
Chairperson/Trustee	**Principal Officer**	**Trustee**
Date	Date	Date

Annexure A

Glossary

Term	Acronym	Definition
Biometrics	--	A technique of personal identification that is based on physical, physiological or behavioural characteristics including blood type, fingerprints, DNA analysis, retinal or iris scanning, and voice recognition.
Breach	--	A confirmed incident in which personal information was compromised, lost, destroyed, altered, and/or exposed to or processed by unauthorised individuals or entities, and which requires notification procedures in terms of our contractual obligations and/or POPIA.
Child	--	A person under the age of 18 years who is not legally competent to take any action or decision in respect of him- or herself without the assistance or consent of a parent, guardian or similar competent person.
Confidentiality	--	The information security principle that information is not made available or disclosed to unauthorised individuals or entities. May also be referred to as privacy.
Consent	--	Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Control	--	A measure put in place to manage risk.
Data Subject	--	A natural person (individual) or juristic person (legal entity) to whom personal information relates or who can be identified by such information.
De-identify	--	Delete or destroy personal information that identifies a data subject, can be used or manipulated to identify them, or that can be linked to other information that identifies them.
Direct marketing	--	To approach a data subject (in person, by mail, or by electronic communication) for the purpose of promoting or offering to supply goods or services, or to request a donation of any kind for any reason.
Effective date	--	The date from which this policy becomes implementable and enforceable.
Guidelines	--	Information or advice on how to act or the controls that should be used in a specific scenario or situation, covering recommendations or best practice to provide additional detail or further context. Guidelines are typically recommended but not mandatory.
Incident	--	An identified occurrence of an adverse event, indicating a breach of policy, control failure, or previously unknown situation that may have an impact on the privacy or data protection responsibilities of the organisation. Some incidents may become breaches once confirmed or investigated.
Information Officer	IO	An individual contemplated by POPIA and PAIA who is responsible for implementing and overseeing measures to give effect to the conditions for the lawful processing of personal information, and ensuring that the organisation complies with its obligations in terms of POPIA and PAIA.
Information Regulator	IR	The regulatory body established by section 39 of POPIA, and who has oversight and authority over POPIA and PAIA.
Integrity	--	The information security principle that describes the accuracy and completeness of information, and the assurance that it is not compromised by unauthorised modification.
Minimality	--	The use of only the smallest subset of personal information needed to perform and activity, fulfil a duty, or achieve a purpose related to its collection.
Operator	--	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, i.e. a person or organisation that is a separate legal entity to the Fund.
--	PAIA	The Promotion of Access to Information Act 2 of 2000, as amended, and its Regulations.

Term	Acronym	Definition
Personal Information	PI	As defined by POPIA, personal information is information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to— (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person, (b) information relating to the education or the medical, financial, criminal or employment history of the person, (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person, (d) the biometric information of the person, (e) the personal opinions, views or preferences of the person, (f) 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, (g) the views or opinions of another individual about the person, and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
Processing	--	Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including— (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use, (b) dissemination by means of transmission, distribution or making available in any other form, or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information.
Public body		Means- *a)* any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or *b)* any other functionary or institution when— (i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or exercising a public power or performing a public function in terms of any legislation.
Record	--	Any recorded information— (a) regardless of form or medium, including any of the following: (i) Writing on any material, (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored, (iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means, (iv) book, map, plan, graph or drawing, (v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced. (b) in the possession or under the control of a responsible party (c) whether or not it was created by a responsible party, and (d) regardless of when it came into existence.

Term	Acronym	Definition
Responsible Party	RP	A public or private body who alone, or in conjunction with others, determines the purpose of and means for processing personal information.
Restriction	--	To withhold from circulation, use or publication and personal information, but not to delete or destroy such information.
Risk	--	A measure of the extent to which personal data and information is threatened by a potential event, circumstance or occurrence.
Special personal information	SPI	As defined by POPIA, more sensitive categories of personal information which may not be processed unless certain conditions are met and/or more stringent security controls are applied, including: (a) religious or philosophical beliefs, (b) race or ethnic origin, (c) trade union membership, (d) political persuasion, (e) health or sex life, (f) biometric information, (g) the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence, or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings, and (h) the personal information of children.
Standards	--	A document that provides specific and more detailed mandatory controls that help to enforce and support policies, establishing the minimum requirements necessary to drive consistent embedding and behaviour. Standards may be based on external best or acceptable practice or an internal view of minimum requirements.
Third party service provider	--	See definition for “Operator”.