PRIVACY POLICY

DHL Provident Fund
(Registration Number 12/8/36179/1)
Effective Date 1 July 2021

Table of Contents

1. Introduction

As a registered South African entity, The DHL Provident Fund, Registration Number 12/8/36179/1 ("the Fund") is required to comply with the Protection of Personal Information Act 4 of 2013 (POPIA).

The Fund is committed to privacy and the protection of all Personal Information ("PI"). As required in terms of POPIA, the Fund has appointed an Information Officer ("IO") and agreed the duties and responsibilities of the IO as set out in item 3 of this policy.

The Fund acknowledges that it is a Responsible Party in terms of POPIA and makes use of Operators to process PI where contracts are in place setting out the following:

- Authorisation of the processing of PI.
- All PI held by Operators is treated as confidential and shall not be disclosed unless required by law or during the performance of its duties.
- The necessary security safeguards are implemented and maintained per Section 19 of POPIA.
- The Operator must immediately notify the Fund where there are grounds to believe that PI has been breached in any way.
- The Operator undertakes to assist the Fund in meeting its obligations in terms of POPIA.

The Fund:

- Will establish measures to adhere to all applicable codes of conduct and/or industry regulations. In the event of any conflict, any code of conduct recognised by law and applicable to retirement funds and their service providers will prevail.
- Recognises that privacy and data protection is an ongoing requirement and will require regular supervision and revisions to policies and procedures.
- Undertakes to strive for ongoing compliance.
- Will require that any new initiatives, activities, products, service providers which impact the safeguarding of PI, will consider data protection and privacy requirements during assessment.

2. Purpose and applicability of the Privacy Policy

The aim is to set 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 compliance.

Appropriate governance, management and oversight activities will be established to ensure that suitable measures, controls and standards are implemented to ensure compliance; this upholding the inherent rights of Data Subjects.

The Trustees, service providers, contractors, third parties and any other officers of the Fund involved in the processing of PI on behalf of the Fund are bound by this Policy.

3. Duties and Responsibilities of the Information Officer

In accordance with POPIA, The Fund is required to either appoint an IO (and as appropriate, deputy Information Officer/s), or, the "head of the fund" is appointed by operation of the Act, to oversee and supervise compliance.

As set out in section 55 (1) of POPIA, an IO is required to:

- Encourage Trustees of a fund to comply with the eight conditions for the lawful processing of PI.
- Deal with requests made to the trustees of a fund under the Act.
- Work with the Information Regulator if there is an investigation into the trustees or a fund in terms of Chapter 6 of the Act (providing for the processing of personal information, subject to prior authorisation by the Information Regulator).
- Ensure compliance by the fund with the Act.
- Comply with any other duties and responsibilities which may be prescribed.

In terms of the Regulations issued in 2018, in addition to the responsibilities referred to in section 55(1) of the Act, an IO:

(1) Must ensure that-

(a) a compliance framework is developed, implemented, monitored and maintained

(b) a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of PI;

(c) a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

(d) internal measures are developed together with adequate systems to process requests for information or access thereto; and

(e) internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.

(2) Must provide copies of the manual (Promotion of Access to Information Act 2 of 2000 (hereinafter referred to as "PAIA")/POPIA manual), to a person who has requested same, subject to payment of a fee to be determined by the Regulator from time to time.

3.1 Purpose

- Confirm the process for the appointment of the Fund's Information Officer (and where appropriate Deputy Information Officer/s).
- Summarise the various duties and responsibilities of the Information Officer identified by the Fund.
- The Act requires the appointment of an IO and enables the appointment of one or more deputy IO's.
- The Fund is required to ensure that the appointed IO and Deputy IOs register with the Information Regulator. Once the registration process has been completed, the said officers are required to confirm to the Board that they have complied with the registration process.

3.2 Delegation to Deputy Information Officer/s

In terms of section 56 of the Act the IO may delegate, in writing, any of the functions and duties in terms of the Act to a Deputy IO/s. The Information Officer may amend and/or revoke the delegation, in writing, at any time. A copy of the delegation document must be provided to the Board of Trustees.

Any decision of the Deputy IO shall be regarded as a decision of the IO, unless, the IO has stipulated that any decision must be referred to him/her for ratification.

Regardless of any delegation, the IO shall retain full responsibility for any function or duty delegated to the Deputy IO/s.

3.3 Termination

The IO and Deputy IO/s may terminate his/her appointment by giving 30-days written notice.

3.4 Services to be Provided by the IO

The IO is required to perform the legislative functions as set out in the Act, in conjunction with relevant regulations, codes of conduct, information circulars as may be issued by the Information Regulator from time to time, and as set out in this document. Such legislative functions shall include any regulatory returns, reports, and notifications.

Carry out the statutory duties allocated to the IO, any other functions delegated by the Board to ensure further compliance with the Act and the principles contained in the Act, which includes:

- Assist the Board by arranging training regarding the provisions of the Act, regulations, codes of conduct and information made available by the Information Regulator
- Develop a compliance framework, including an implementation plan and ongoing review plan that takes account of amongst others:
    - The relationship between the Fund, the Employer, the appointed section 13B of the Pension Funds Act, 1956 (as amended) licensed administrator, any statutory appointments made by the Fund, and any other service provider appointments
    - The principle of minimality
    - Identifying the purposes for which all information is collected
    - Record management and retention schedules
    - Communication to Fund Members regarding their rights
    - Communication to the Employer regarding its obligations
    - The obligations of the Board of Trustees regarding PI they access and reasonable security safeguards to use
    - Breach notification procedures to apply to the Fund, operators and service providers
    - Breach notification procedures to notify the Information Regulator and affected Fund Members.
- Devise a process to monitor compliance within the developed framework.
- Develop the necessary privacy policies, registers, and any other documents required to execute the compliance implementation and review plan.
- Undertake a personal information impact assessment to ensure that adequate measures and standards exist in order to comply with the lawful conditions for the processing of personal information.
- Engage and correspond with all service providers regarding compliance with the framework and information required to complete the personal information impact assessment.
- Engage and correspond with the Employer regarding compliance with the framework and information required to complete the personal information impact assessment.
- Review the Fund's service level agreements with service providers and ensure they are updated to comply with Act, regulations and codes of conduct. This may include a Data Processing Agreement.
- Review all existing governance policies and documents and make recommendations to the Board on revisions required to ensure compliance with the framework and privacy policies developed.
- Develop and maintain a manual as required in terms of PAIA, including content required in terms of the Act and, as applicable, by the Information Regulator.
- Liaise with data subjects regarding all requests related to the Act and Regulations to the Act published in 2018 and PAIA.
- Maintain a register of objections to processing of PI received and the response to the data subject provided by the IO.
- Maintain a register of requests for deletion of PI and the response to the data subject provided by the IO.
- Maintain a register of requests made in terms of PAIA, a complaints register and a breach register.
- Engage and assist the Information Regulator on complaints, pre-investigation processes, settlements, conciliation, assessment and other supervisory and enforcement processes enabled in terms of the Act.

3.5 Consent and Collecting Consent

Assist the Board in determining whether consent is required from data subjects and to develop mechanisms to obtain, record and store consent obtained.

3.6 Compliance with any other Data Protection Laws

Assist the Board in determining whether any other data protection laws may apply, for example, the General Data Protection Regulation ("GDPR") regulations on data protection and privacy applicable in the European Union and to recommend compliance practices to incorporate in the compliance framework to specifically address compliance, and, importantly, breach protocols.

3.7 Engaging experts to assist in executing the services to be provided by the IO

The IO is authorised to engage experts and/or service providers to assist in executing the services to be provided as set out in this document subject to the authorisation requirements related to costs and charges applicable.

3.8 Reporting to the Board Annually on Compliance with the Act

The IO will annually report to the Board on compliance with the Act, with reference to the registers that are required to be maintained and in particular non-compliance identified, and corrective measures required to be implemented.

3.9 General

The IO will:

- Annually review the level of data protection and cybercrime cover maintained by all service providers and advise the Board should the IO have any concerns related to a service provider.
- Annually review whether the Fund should adjust the data protection and cybercrime cover it maintains.

4. Policy Statements: Conditions for the lawful processing of PI

The Fund is accountable for ensuring that the conditions for lawful processing are complied with. 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.

4.1 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"). In terms of section 13A of the Act, the Fund is obligated to receive payment of contributions and schedules detailing PI from the employer/s that participate in the Fund.

The employer/s is obligated in terms of the Act and the Income Tax Act 58 of 1962, as amended, ("ITA") to ensure that eligible employees, are entered as Fund members as a condition of their employment. The employer/s is required to advise the Fund when the service of an employee is terminated.

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 is committed to:

- The Fund will collect and process PI in compliance with the obligations prescribed in POPIA;
- Protect the legitimate interests of Data Subjects as Fund members;
- Uphold, as far as is reasonably possible, the principle of minimality – where only adequate, relevant, and necessary data and/or information is processed to achieve the required purpose;
- Develop and communicate processes to enable Data Subjects to
    - Object, where reasonable and lawful, to the processing of their Personal Information; and
    - Request that their PI be updated or corrected; and
    - Request, where legally feasible, the deletion of PI or to restrict processing and access to the PI.

4.2 Purpose Specification

The Fund will establish measures to:

- Ensure PI is only used for the purpose/s for which it is collected; and
- Notify Data Subjects of the purposes for which the Fund collects and processes their PI. To achieve this, the Fund has developed a Privacy Statement that is made available to all new entrants and will accompany the Member booklet issued to all Fund members.

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. Further, Section 14(5) of the Act requires that PI under the Fund's control be destroyed or deleted in a manner that prevents its reconstruction in an intelligible form.

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 Fund has concomitantly formulated a Records Register which details the storage, retention and deletion register of records.

The Fund has contracted with several Operators (third party service providers), including a licensed administrator, based on their skills and ability to render specified services to the Fund. Such Operators will be required to adhere to the Records Register.

In terms of this Record Register:

4.2.1 Purpose Specification

The classification to apply is detailed below; this list of examples is not exhaustive:

Level	Examples	Guidance
Public	- Registered rules - Audited annual financial statements - PAIA Manual	Required to be submitted to the Financial Sector Conduct Authority and in consequence is available to the general public. Submitted to South African Human Rights Council and in consequence is open for inspection.
Internal	- Agendas for, and minutes of, Board meetings held - Governance policies, procedures, practice notes, and registers - Communication to stakeholders - Correspondence with stakeholders, the Authority 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 the Act.	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.

Level	Examples	Guidance
Sensitive	Special Personal Information as defined in the Act (e.g. 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.

4.2.2 Principles Regarding Lifecycle of Documents and Records

The lifecycle of documents and records includes the entire process flow of the collection, creation, processing, storage, access, use, disclosure (or communication, transmission, sharing, retention, archiving, deletion and destruction 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 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 Information Officer for deletion and destruction, or deleted/destroyed as instructed by the Information Officer,
- 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, an
- Will not be duplicated or retained indefinitely, unless authorised by the Information Officer.

4.2.3 When a Trustee and/or Fund Officer Leaves Office

- All paper documents and records must be returned to the Information Officer for deletion and destruction. The Information Officer 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.

4.2.4 Data Storage, Retention, Deletion and/or Destruction

The Trustees and Fund officers require that all documents and records listed in the documents and storage register:

- 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 above, provided that the Information Officer 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.

4.3 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:

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

4.4 Quality of Information

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

- Engage with Employer/s, as the primary source of information, to assist in ensuring that PI processed is updated to be accurate, complete, and not misleading.
- 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.

4.5 Openness

The Fund will include in its Communication Policy, specific communication to notify Fund members of their rights in terms of POPIA, that they are able to lodge a complaint with the Information Regulator and the contact details of the Information Regulator.

As the Fund contracts with several 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 is implicated in a complaint, the following will apply:

- The IO will circulate a copy of the complaint to the Board within 5 working days of receipt of the notification from the IR;
- The IO will engage with the office of the IR as set out in the "Roles and responsibilities of Information Officer" document;
- As necessary, the IO will request the Board's assistance in the complaint resolution process; and
- 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 Fund's Complaints Register, include the register at each formal meeting and report to the Board on recommendations in improving processes, measures, controls and standards applicable to minimise/better manage a reoccurrence of the complaint.

4.6 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 unauthorized person ("an information breach" or "compromise"), the Fund is required to notify the IR and the affected Data Subjects:

- As soon as reasonably possible after the compromise, and
- Such notification must include the following:
  - information about the compromise;
  - 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:

1. **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 on systems containing PI or Fund data;
   - Unauthorized sharing of information by a third party or a cyberattack on a third party who has received or has control over PI or Fund data.

2. **Assessing the severity of the breach**

   The assessment scoring system to be used to determine the Severity Rating of the compromise has been developed. While each compromise will/ may be different, the following input factors should be considered:

   - The number of Data Subjects impacted;

- 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;
- Likely impact to the Data Subjects and/or the Fund;
- Likely financial loss that the Fund could be exposed to, including any fines that may be imposed
- 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	Assessment
Low	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
Medium	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
High	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

3. Investigating the breach

When the IO has assessed the compromise and assigned same a Severity Rating, a root cause analysis must be conducted to determine:

- The Severity
- Remediation available;
- The most appropriate remediation response given the nature of the compromise;
- The potential costs of remediation and communication;
- What measures Data Subjects could take to protect themselves and how the Fund would be able to assist;
- 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.

On receipt of the report, the Chairperson will advise the Crisis Communication Committee to initiate the communication response to stakeholders including the IR. The Chairperson is responsible to ensure that the Crisis Communication 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.

4. **Breach reporting**
   The IO will complete the breach register following every compromise investigation and report issued. The Fund maintains a breach register.

4.7 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 the Promotion of Access to Information Act 2 of 2000 (PAIA). The Fund has directed the IO to update 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:

- Engage with the Employer/s, as the primary source of information and co-Responsible Party, to assist Data Subjects with requests to correct or update their PI; and
- Contract with its service providers to require that processes be established to assist Data Subjects with requests to:
  - 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).
  - correct or update their PI. This may include making mechanisms available to Data Subjects to access and update their own information.

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.

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:

- A data Subject who wishes to object to the processing of Personal Information must submit the objection using Form 1
- A data Subject who wishes to request the deletion of Personal Information must submit the request using Form 2

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 request, reasons for request and response to the Data Subject. These registers are maintained by the Fund.

4.8 Special Personal Information

Whenever categories of Special Personal Information (e.g. 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:

- As far as possible and practical, the Fund will keep records of access to all Special Personal Information.
- 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.

4.9 Direct Marketing

The Fund, and by extension its service providers and third parties will not actively engage in direct marketing activities related to the products and services provided by the Fund, if applicable. Accordingly, the Fund's service providers will not be authorised to use any PI of Fund members for their own direct marketing purposes.

4.10 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 (e.g. 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.

4.11 Transborder Information Flows

The Fund adheres to the requirements stipulated in POPIA for the transmission of Personal Information across international borders, where and if this is a requirement.

4.12 Regulatory Authorisation

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

4.13 Personal Information Impact Assessment

The IO 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 Personal Information.

The IR or the Act does not provide detailed guidelines on performing PIIAs. Accordingly, the Fund has developed a PIIA framework that will allow an initial assessment of its compliance, and thereafter, regular rigorous assessment of the risks will be completed.

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, any guidelines issued, and other changes, for example, to the Fund's information processing operations, service providers, technology and/or subject to market changes which may affect the Fund.

PIIA Process:

1. Identify risks

The Fund will:

- Determine the categories of risk it wishes to evaluate itself against.
- 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 Personal Information. At a minimum, the Inventory is aligned to the records listed in the Fund's PAIA Manual.

2. Evaluate Risks

The Fund will:

- For each of the risks identified in the first step, determine the level of risk (risk rating) per item.
- 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.
- Take into account several factors to consider in evaluating risk.

Risk factors: factors taken into account when rating risk related to fund activities:	
1	The number of *different personal information types or uses* indicated for that activity in your diagrams and tables. This automatically includes whether the party is processing: (a) the different types of special personal information (b) personal information leaves the country (d) account numbers are processed (c) children's information is processed
2	How *much* personal information is being processed.
3	How *often* personal information is being processed.
4	The *duration* of the processing.
5	The *number of data subjects* involved in the processing.

RISK RATING OF HIGH-LEVEL FUND ACTIVITIES THAT INCLUDE THE PROCESSING OF PI		
Activity	**Processing activity**	**Personal information processed**
1.	Board members and other fund officers – appointment, election, ongoing fit and proper requirements, evaluation, and removal i.e., "***board member data"***	Full names, identity number, date of birth, nationality, occupation, residential address, business address, postal address and date of appointment, conflicts and declarations of interest, board memberships, in some cases other employment or provisions of services information and remuneration information, training, education, qualifications, experience, fit and proper requirements information, criminal record, professional body membership and disciplinary information, telephone numbers, email addresses, name of employer, directorships, prescribed person information, FICA information, reasons for removal from office
2.	General – many activities performed by the fund's board related to the fund's operations and investments and this will include fund information and membership data. "***membership data"*** is specified in the next column (excluding nomination of beneficiary information)	Records of the operations of the fund. Including: membership records with details and dates of joining and leaving the fund, members' identity or other numbers, dates of birth, age, nationality, retirement age, members' employment capacity, occupation or level of employee, employee numbers, employer details, including name, registration number, FICA information, paypoints, contact persons, persons responsible for contributions, directors details, employer and member information prescribed by the FSCA, members' contact details, including cell phone numbers and addresses, contributions received, contributions statements from employer including remuneration, pensionable salary, taxable salary, cost to company information, tax numbers, leave record, reason for leaving employment, premiums paid in respect of insured benefits (e.g. death and ill health), movement of investments, assets receipt or payment of money or assets in respect of transfers in and out, member's minimum individual reserves or

		accounts, employment status and reasons for leaving employment; health and disability information, reports and records related to a disability member, divorce and maintenance information and orders (including information contained therein about ex-spouses, partners, ex-partners, living arrangements, spouses, family and children), unclaimed benefits, housing loans and guarantees by fund and other financial service providers to members, housing purchases and building projects of members. Trade union, bargaining council or employer association information. Details of immoveable property/residence of members or members' spouse, mortgage over property and/or pledge of members' benefits, terms of loan repayment and default. Medical aid or medical aid subsidy information.
3.	Payment of benefits (excluding (i) lump sum death benefits and (ii) deductions and withholding which are dealt with separately below): benefit payments made to a member leaving the fund other than on transfer, for example on withdrawal, death or retirement.	Membership data, Elections regarding payment of benefits, Members financial advisor details, Tax payable with respect to member, tax directives and applications, PAYE, knowledge of members' tax affair e.g., if they are not in order, Bank account details
4.	Administration of contributions, including receipt and allocation to investments, monitoring, reporting, allocation to fund expenses and risk benefits – of both member and employer contributions	Membership data. Reports of non-compliance by employer related to contributions and contributions statements. Information about litigation or reporting of employers to SAPS, members, the board and FSCA. Employer's defense. Knowledge of and action related to criminal offences of employer and persons at the employer related to section 13A of the Pension Funds Act.
5.	Investment strategy, administration, and management	Membership data
6.	Management of fund-owned insured benefits and policies	Membership data
7.	Benefit statements and benefit projection statements provided to members and previous members	Membership data
8.	Lump sum death benefits – payable by the fund under section 37C of the Pension Funds Act – investigation as well as allocation and payment decisions	Membership data. Nomination of beneficiary data (see below). Beneficiary information: name, identity numbers, address and other contact information, relationship to deceased, ability to look after financial affairs, financial literacy, banking records, employment status, occupation, financial (assets and income statements), children, family members, living arrangements, account numbers and details, criminal behavior, divorce and maintenance information, partner, spouse and ex-partner and spouse information, caregiver, health, medical records, life expectancy information, education, training, age, identity number, longevity, sex-life, paternity tests. Other information required to determine dependency.
9	Decisions to withhold or deduct from benefits – in terms of section 37D of the Pension Funds Act with respect to compensation for damage caused to the employer by the member	Membership data. Misconduct at employer, allegations and reports, including forensic reports form employer. Litigation, compensation and other legal claim (including CCMA) information of employer and member. Reporting of criminal activity by employer to SAPS. Action by SAPS or NPA against members. Criminal activity, theft, fraud, misconduct, dishonest behaviour of members. Disciplinary proceedings against members. Information about financial prejudice to members, including family and details about other income sources and financial information.

10.	Nomination of beneficiaries by members i.e., member's ***"nomination of beneficiaries data"***	Membership data. Names, identity numbers, percentage nomination of member's children, spouses, partners, parents, siblings, other family members, important others, relationship to member, sex-life information.
11.	Actuarial and valuation activities, including reporting	Membership data. Board member data.
12.	Financial statements and prescribed reporting	Membership data. Board member data.
13.	Requests for information and complaints	Membership data. Board member data. Upon divorce and maintenance queries with respect to member: member's representatives, fund name and registration number, membership of the fund, minimum individual reserve or account information, pension interest amount, housing loan information, children, spouses, partners, ex-spouses and partners personal information and their representatives.
14.	Establishing, registration, termination, liquidation of fund and transfers in and out of the fund, surplus apportionments, and conversions.	Membership data. Board member data. Data relating to former members.
15.	Appointment, contracting and termination of service providers, appointees, agents and ongoing monitoring and reporting of service providers- provider information	Membership data. Board member data. Information of service providers: company name, company registration numbers, FICA information, due diligence information, including previous criminal behavior or other forms of misconduct and fit and proper information, directors and management identity and contact details, legal, compliance and regulatory information, contractual arrangements, errors and omissions, information about claims or litigation, conflicts and declarations of interest, qualifications, licenses, fit and proper requirements information, professional body membership, prescribed information
16.	Meetings, sub-committee meetings, packs, agendas, resolutions, minutes, receiving and storage of fund information	All the above-mentioned information

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

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

Risk Rating	Action
Very Risky	- Start corrective action immediately, to be addressed within next 3 months. - Monitor closely to verify success. - Consider stopping the activity where appropriate/ practical to do so.
Medium Risk	Start corrective action within the next 3 months, to be resolved within the next 6 months. Monitor to verify success.
Low Risk	Take action in line with operational requirements, or review action to be taken within 6-months.

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 maintained by the Fund.

5. 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.

6. Adoption

This Policy is hereby adopted by the Board of Trustees of the Fund:

Chairperson/Trustee	**Principal Officer**	**Trustee**
Date	Date	Date