## Personal Information Impact Assessment

## For Funds

Aligned with conditions for lawfully processing personal information per the Protection of Personal Information Act 4 of 2013 (POPIA), this PIIA should be completed in line with the Privacy Policy requirements.

| | Assessment Area | Description of Risk | Operational / Strategic | Responsibility | Likelihood of Occurrence | | Impact on the Fund | | Risk Rating | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Accountability and Governance | The Fund has appointed an Information Officer to ensure that all compliance and regulatory requirements related to the protection of personal information are met. | Strategic | Board of Trustees | | 0 | | 0 | 0% | |
| 2 | Accountability and Governance | The Fund has ensured adequate POPIA training for the Board of Trustees, Information Officer, employees and consultants to improve understanding of requirements and reduce risks to personal information. | Operational | Board of Trustees | | 0 | | 0 | 0% | |
| 3 | Accountability and Governance | The Fund has registered its Information Officer with the Information Regulator per prescribed guidelines. | Operational | Principal officer | | 0 | | 0 | 0% | |
| 4 | Accountability and Governance | The Fund has drafted a Privacy Policy and other related governance documentation outlining its principles when it comes to handling and securing the personal information that it is responsible for. | Operational | Information officer | | 0 | | 0 | 0% | |
| 5 | Accountability and Governance | The Privacy Policy and related governance documentation are reviewed annually, or whenever there is a significant change that may affect personal information, to ensure alignment with legislation. | Strategic | Information officer | | 0 | | 0 | 0% | |
| 6 | Processing Limitation | The lawful basis for processing personal information by the Fund and its service providers is understood, and does not infringe on the rights of data subjects. | Operational | Information officer | | 0 | | 0 | 0% | |
| 7 | Processing Limitation | Data sets that are collected or processed by or on behalf of the Fund are minimised or redacted to ensure that only the required information to achieve the purpose is processed, and that such processing is not considered excessive. | Operational | Information officer | | 0 | | 0 | 0% | |
| 8 | Processing Limitation | Consent requirements are identified and the Fund maintains a record of such consent (or ensures that one of its service providers does so). | Operational | Information officer / Administrator | | 0 | | 0 | 0% | |
| 9 | Processing Limitation | The Fund has a process or makes allowance for data subjects to object to the processing of their personal information and can facilitate / resolve such objections. | Operational | Information officer / Administrator | | 0 | | 0 | 0% | |
| 10 | Processing Limitation | The Fund acknowledges that while collecting information directly from a data subject is preferable, due to practical considerations it will engage the Employer to provide personal information to its service providers via a well-defined process. | Operational | Information officer | | 0 | | 0 | 0% | |
| 11 | Purpose Specification | The Fund has identified all records of personal information that it processes and recorded the purpose/s for which this information is being processed. | Operational | Information officer | | 0 | | 0 | 0% | |
| 12 | Purpose Specification | Appropriate policies and procedures exist to ensure that records of personal information are retained for the length of time required to fulfil the purpose (e.g. retirement savings and other benefits, compliance, further Fund objectives), following which they are suitably destroyed (physical and electronic). | Operational | Information officer / Administrator | | 0 | | 0 | 0% | |
| 13 | Purpose Specification | Technology and communication devices used by the Fund that contain or have access to personal information processed by the Fund must be appropriately destroyed or sanitised before being repurposed to ensure personal information is not compromised. | Operational | Information officer | | 0 | | 0 | 0% | |
| 14 | Further Processing | The Fund can identify additional purposes for processing personal information beyond the reasons that it was collected and can notify data subjects in the event that such processing is required. | Operational | Information officer / Administrator | | 0 | | 0 | 0% | |
| 15 | Information Quality | The Fund is confident that the quality of data about its members is of a suitable quality to achieve its purposes (i.e. retirement savings and other benefits), both by the Fund itself and at its service providers. | Operational | Information officer / Administrator | | 0 | | 0 | 0% | |
| 16 | Openness | The Fund has drafted a PAIA Manual which includes all requirements from POPIA, and reviews this manual in accordance with their policies and procedures. | Strategic | Information officer | | 0 | | 0 | 0% | |

| | Assessment Area | Description of Risk | Operational / Strategic | Responsibility | Likelihood of Occurrence | | Impact on the Fund | | Risk Rating | |
|---|---|---|---|---|---|---|---|---|---|---|
| 17 | Openness | The Fund ensures that ALL data subjects are aware / have been notified of the processing of their personal information by notifying them of such (either via the Employer or through communications issued by the Fund or service provider). | Operational | Trustees / Employer | | 0 | | 0 | 0% | |
| 18 | Openness | The Fund has established a standard process to deal with any requests for access to personal information made via PAIA, whether by the data subject themselves, or an external party. | Operational | Information officer | | 0 | | 0 | 0% | |
| 19 | Security Safeguards | All Trustees and other stakeholders processing Fund information, including personal information, have appropriate technology controls on their devices (e.g. encrypted hard drives, password protection on laptops and mobile phones, use of secure / encrypted channels for transmitting personal information, restricted access to Fund drives / cloud folders). | Operational | Information officer | | 0 | | 0 | 0% | |
| 20 | Third Party Management | Contractual clauses are included in ALL of its contracts with all of its service providers to ensure that appropriate security safeguards are implemented by these providers when processing personal information on the Fund's behalf. | Operational | Information officer | | 0 | | 0 | 0% | |
| 21 | Third Party Management | The Fund has performed satisfactory risk management / due diligence procedures on service providers processing personal information on its behalf to give it appropriate comfort that this information is protected. | Operational | Information officer | | 0 | | 0 | 0% | |
| 22 | Third Party Management | The Fund has established a standard procedure to receive notification of any data breaches from its service providers, so that the breach can be suitably investigated, contained, reported and resolved. | Operational | Information officer | | 0 | | 0 | 0% | |
| 23 | Data Subject Participation | The Fund has established appropriate processes to enable its members to gain access to their personal information and correct or update it as necessary (e.g. directly with service providers, or via the employer to provide to the service providers). | Operational | Information officer / Administrator | | 0 | | 0 | 0% | |
| 24 | Data Subject Participation | For requests to access and correct personal information, appropriate practices and procedures are in place to verify the identity of an individual before providing them with access to their personal information. | Operational | Information officer / Administrator | | 0 | | 0 | 0% | |
| 25 | Special Personal Information | The Fund identifies any of the categories of special personal information as defined in POPIA (e.g. race, health data, children's information), and protects it with more stringent security safeguards. | Operational | Information officer / Administrator | | 0 | | 0 | 0% | |
| 26 | Direct Marketing | Direct marketing activities are considered and managed by the Fund, and consent is collected for all instances where direct marketing is performed. | Operational | Information officer / Administrator | | 0 | | 0 | 0% | |
| 27 | Automated Decision-Making | Should automated decision-making, profiling, or other algorithms be employed beyond those mandated by law (group insured benefit risk profiling, medical underwriting), the Fund will make provision for data subjects to make representation about such decisions, explain the logic regarding the decision, and allow for appeal to have such a decision reviewed. | Operational | Information officer | | 0 | | 0 | 0% | |
| 28 | Transborder Information Flows | The Fund has understood any transborder flows of personal information and has satisfied itself that such jurisdictions have suitable data protection laws, and/or contractual clauses in service provider appointment contracts in these jurisdictions to ensure protection of the data, and the data is suitably protected at rest and in transit. | Operational | Information officer | | 0 | | 0 | 0% | |
| 29 | Data Breach Management | The Fund has a defined process for managing and investigating breaches, and reporting such events to the Information Regulator. | Operational | Information officer | | 0 | | 0 | 0% | |
| 30 | Data Breach Management | The Fund has a defined process for notifying data subjects in the event that their personal information is compromised or breached. | Operational | Information officer / Administrator | | 0 | | 0 | 0% | |

| | Assessment Area | Description of Risk | Operational / Strategic | Responsibility | Likelihood of Occurrence | | Impact on the Fund | | Risk Rating | |
|---|---|---|---|---|---|---|---|---|---|---|
| 31 | Data Breach Management | The Fund has notified its service providers of its process for breach reporting in the event that personal information processed by these providers is compromised or breached. | Operational | Information officer | | 0 | | 0 | 0% | |
| 32 | Regulatory Authorisation | The Fund confirms that it does not perform any of the following activities, and if it does, that it will apply to the Information Regulator for authorisation to continue these activities:<br>- Processing unique identifiers (e.g. SA ID Number) to link personal information together with information from other responsible parties for a purpose other than that considered when collecting such identifiers.<br>- Processing information on criminal behaviour or unlawful or objectionable conduct on behalf of third parties.<br>- Processing information for the purposes of credit reporting.<br>- Transferring special personal information or children's information to a third party in a country that doesn't have an adequate level of protection. | Operational | Information officer | | 0 | | 0 | 0% | |
| 33 | Personal Information Impact Assessments | The Fund performs this Personal Information Impact Assessment at least annually to understand its compliance risks and the risks to personal information in the Fund's care or under its control. | Operational | Information officer | | 0 | | 0 | 0% | |
| 34 | Industry Regulations | The Fund monitors changes to industry regulations and codes of conduct which may pertain to the Fund in terms of the processing and protection of personal information. | Operational | Information officer | | 0 | | 0 | 0% | |
| 35 | Privacy by Design and Default | The Fund ensures that all new initiatives, activities or products consider data protection requirements at the outset of such initiatives to ensure that mandatory compliance requirements, security and/or privacy controls are implemented and active by default to protect a data subject's rights. | Operational | Information officer | | 0 | | 0 | 0% | |