OPFA POPIA POLICY & DATA PRIVACY CONSENT NOTICE

Title:	OPFA: POPIA Policy and Data Privacy Consent Notice
Custodian:	Information Officer/Deputy Information Officer
Prepared By:	Senior Legal Advisor
Date Created:	February 2021
Version No:	V2
Reference No.	TBA
Date Approved:	18 March 2024
Effective Date:	Date of Accounting Authority Approval
Approved By:	Accounting Authority

Document owner:

NAME	POSITION
Nondumiso Ntshangase	Deputy Information Officer

Mandatory Review period:

To be reviewed every second year or when significant changes occur

Version Control Page

This page should provide a history of previous versions of the policy and changes made:

Version	Date	Author	Status	Comment / changes
1	01/02/21	OPFA ManCo	Approved	First version
2	18/03/24	OPFA ManCo	Reviewed and Approved	Minor updates.

The Office of the Pension Funds Adjudicator

(hereinafter referred to as “the OPFA”)

POLICY ON DATA PRIVACY AND THE PROTECTION OF PERSONAL INFORMATION

The Protection of Personal Information Policy establishes, explains and sets out-

- Legal requirements relating to Personal Information and Data Privacy;
- What is Personal Information and who it belongs to;
- What Personal Information will be processed by the OPFA;
- Why the OPFA needs to process a Data Subject’s Personal Information;
- What the OPFA will be doing with a Data Subject’s Personal Information;
- Who the OPFA will share a Data Subject’s Personal Information with;
- What the OPFA will do with a Data Subject’s Personal Information, once the purpose for the processing comes to an end;
- How everyone at the OPFA are to treat Personal Information belonging to another.

Table of Contents

1. Introduction

The Protection of Personal Information Act, 4 of 2013 (POPIA) regulates and controls the processing of Personal Information.

The OPFA is established in terms of section 30B of the Pension Funds Act 24 of 1956. The main object of the OPFA is to dispose of complaints lodged in terms of section 30A (3) of the Pension Funds Act in a procedurally fair, economical and expeditious manner.

The OPFA for the purposes of carrying out its business and related objectives, does and will from time to time, process the Personal Information of living individuals and legal entities, including public and private entities, such as Personal Information relating to employees and staff, prospective employees and job applicants, students and interns, service providers and contractors, vendors, complainants, parties to a complaint, and other third parties.

The OPFA is a public body as determined in POPIA and is allowed to process personal information while exercising and performing its powers, duties, and functions in terms of the requirements set in the Pension Funds Act, Nr 24 of 1956 ("PFA"), in accordance with POPIA and the PFA regulations regarding the processing of personal information. This applies to the OPFA's functions in relation to disposing of a complaint i.e., it does not relate to other business functions such as corporate support and human resources.

POPIA does not apply to the judicial functions performed by the OPFA. In exercising its powers, duties, and functions under the PFA, in the course of disposing of complaints in terms of Chapter VA of the Pension Funds Act, 1956, the OPFA fully embraces the principles and objectives of POPIA when disposing of complaints, insofar as it may be reasonably practical to do so. Given the importance of privacy, the OPFA is committed to effectively managing Personal Information in accordance with the provisions of POPIA.

The OPFA is obligated to comply with POPIA, and the data protection conditions set out under POPIA with respect to the processing of all and any Personal Information. POPIA does not apply to the judicial functions performed by the OPFA in the course of disposing of complaints in terms of Chapter VA of the Pension Funds Act, 1956. Notwithstanding, and insofar as it may be reasonably practical to do so, the OPFA fully embraces the principles and objectives of POPIA when disposing of complaints. The measures implemented by the OPFA to do so are set out in the OPFA policies pertaining to Personal Information, including this policy.

This Policy describes how the OPFA will discharge its duties to ensure continuing compliance with POPIA in general and the information protection conditions and rights of Data Subjects.

2. POPIA references

To understand the implications of this Policy and the objectives of POPIA the reader must take note of the following POPIA definitions, which will be used throughout this POLICY and which may be used in the interpretation of this document.

POPIA makes use of certain references, as explained below.

"*biometrics*"	means a technique of personal identification that is based on physical, physiological or behavioral characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;
"child"	means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him-or herself;
"competent person"	means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;
"consent"	means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Information;
"Data Subject"	means you, the person, subject to the exemption in respect of the mandate referred to hereinafter, who will provide the OPFA or its Operator/s with Personal Information and who consents when providing such Personal Information, to the OPFA's use thereof in accordance with its Data Privacy Consent Notice. The OPFA is exempted from compliance with the conditions set out in POPIA in fulfilling its mandate in respect of the adjudication of a complaint, as contemplated in section 30G of the Pension Funds Act, 1956.
"Operator"	means a natural person or a juristic person who processes your / a Data Subject's Personal Information on behalf of the OPFA in terms of

a contract or mandate, without coming under the direct authority of the OPFA;

"person" means a natural person or a juristic person;

"Personal Information" means information relating to any identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, namely the Data Subject, including, but not limited to-

- 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;
- Information relating to the education or the medical, financial, criminal or employment history of the person;
- Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other assignment to the person;
- The biometric information of the person;
- The individual opinions, views or preferences of the person;
- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- The views or opinions of another individual about the person;
- 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;

"*parties to a complaint*" means those persons referred to in section 30G of the Pension Funds Act, 1956.

"processing" means any operation or activity or any set of operations, whether by automatic means, concerning Personal Information, including-

- The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
- Dissemination by means of transmission, distribution or making available in any other form; or

- Merging, linking, as well as restriction, degradation, erasure or destruction of information;
- Sharing with, transfer and further processing, to and with such information.

"record" means any recorded information, regardless of form or medium, including any of the following:

- Writing on any material;
- 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;
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph or drawing;
- Photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced;
  - In the possession or under the control of a responsible party;
  - Whether it was created by a responsible party; and
  - Regardless of when it came into existence;

"Responsible Party" means the OPFA including without detracting from the generality thereof, the Adjudicator, Deputy Adjudicator, management, executives, HR practitioners, payroll department, core benefits provider, medical aid department, retirement funding department, internal auditors, legal practitioner and compliance officers, company secretary, and all other employees and Operators who need to process your / a Data Subject's Personal Information for the OPFA.

"Special Personal Information" includes any information relating to an individual's-

Ethnicity, Gender, Religious or other beliefs, Political opinions, Membership of a trade union, Sexual orientation, Medical history, Offences committed or alleged to have been committed by that individual, Biometric details, and Children's details.

"you" means the person who is reading this POLICY and Data Privacy Consent Notice, namely the Data Subject, who by providing the OPFA with your Personal Information, gives the OPFA and its Operators consent to use and process your Personal Information in accordance with the provisions of said Data Privacy Consent Notice, and the word "your / yours" bears a corresponding meaning as the context may indicate.

3. Purpose and Objectives

3.1 The OPFA collects and processes Personal Information belonging to Data Subjects and/or parties to a complaint on an ongoing basis to carry out and pursue its object. This may without detracting from the generality thereof include:

3.1.1 recruitment and employment purposes;

3.1.2 concluding contracts and business transactions;

3.1.3 for risk assessments, insurance and underwriting purposes;

3.1.4 assessing and processing queries, enquiries, complaints, and/or claims;

3.1.5 conducting criminal reference checks and/or conducting credit reference searches or verification;

3.1.6 confirming, verifying and updating persons details;

3.1.7 for purposes of personnel and other claims history;

3.1.8 for the detection and prevention of fraud, crime, money laundering or other malpractice;

3.1.9 conducting market or customer satisfaction research;

3.1.10 promotional, marketing and direct marketing purposes;

3.1.11 financial, audit and record keeping purposes;

3.1.12 in connection with legal proceedings;

3.1.13 providing services to clients to carry out the services requested and to maintain and constantly improve the relationship;

3.1.14 communicating with employees, third parties, customers, suppliers and/or governmental officials and regulatory agencies; and

3.1.15 in connection with and to comply with legal and regulatory requirements or when it is otherwise required or allowed by law.

3.2 The objective and purpose of this Policy is therefore to set out the OPFA's policy on the processing of Personal Information and to provide guidelines on how Personal Information is to be processed and safeguarded to ensure compliance with POPIA.

4. Application and Scope

4.1 This Policy will apply to the processing of all and any Data Subject's Personal Information by the OPFA.

4.2 This Policy, without exception, will apply to:

4.2.1 The OPFA, including all employees thereof, including permanent, fixed term, and temporary staff, the Adjudicator, Deputy Adjudicator, and interns;

4.2.2 Any entity or person who processes Personal Information on behalf of the OPFA, whether residing or operating in South Africa, or overseas, who will hereinafter be referred to as an "Operator", provided they have been made aware of this Policy.

5. The Data Protection Principles and Conditions

5.1 Any employee or Operator who processes Personal Information belonging to a Data Subject on behalf of the OPFA, shall comply with all the provisions of POPIA, or shall comply with the provisions of the OPFA's policies (which can be made available on request) relating to personal information in respect of parties to a complaint, including the 8 data protection conditions set out under section 4 of POPIA, which are as follows:

5.1.1 Personal Information shall be obtained and processed fairly and lawfully;

5.1.2 Personal Information shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes, unless specific consent to do so has been obtained;

5.1.3 Personal Information shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;

5.1.4 Personal Information shall be accurate and, where necessary, kept up to date;

5.1.5 Personal Information processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;

5.1.6 Personal Information shall be processed in accordance with the rights of data subjects under POPIA;

5.1.7 Appropriate technical and organisational safeguards and measures must be put in place to protect and guard against unauthorised or unlawful processing of Personal Information and against accidental loss or destruction of, or damage to, Personal Information;

5.1.8 Personal Information shall not be transferred outside South Africa to another country unless that country has similar Data Privacy laws to those set out under POPIA in place, or the person to whom the Personal Information is being transferred provides a written undertaking to apply the principles set out under POPIA to the processing of the Personal Information.

6. How Personal Information is Processed and Used

6.1 Before any Personal Information is processed, the person processing such information on behalf of the OPFA must bring to the Data Subject's or party to a complaint's attention the provisions set out under the OPFA's consent to process personal information in terms of the tacit consent document, which is set out on the OPFA website, and which for ease of reference is attached hereto marked Annexure "A", which document amongst others houses the following instructions and details:

- Why the processing of the Data Subject's or party to a complaint's Personal Information is necessary,
- What Personal Information is required and the purpose for the requirement;
- What will be done with the Personal Information;
- That in order to use the Personal Information, consent for such processing should be provided, unless such processing is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is a party; or is required and complies with an obligation imposed by law on either the Data Subject or the Responsible Party; or is necessary to protect the legitimate interest(s) of the Data Subject or the Responsible Party; or is necessary for the proper performance of a public law duty by a public body; or is necessary for pursuing the Data Subject or the Responsible Party's legitimate interests, or that of a third party to whom the Personal Information is supplied; or is Personal Information relating to a party to a complaint processed in the course of disposing of complaints in terms of Chapter VA of the Pension Funds Act, 1956.
- Who the Personal Information will be shared with;
- Whether the Personal Information will be sent outside the borders of South Africa and what data security measures are in place to protect the information;
- What will be done with the Personal Information once the purpose for its collection and use has expired.

6.2 When processing a Data Subject's Personal Information, the person processing such information must ensure that:

- They only process Personal Information, which is relevant and accurate and only for the purpose for which it is required;
- Special Personal Information will only be processed in line with the provisions set out under POPIA and in accordance with instructions set out by the Information Officer from time to time.

7. Safeguarding Personal Information

7.1 All OPFA employees and where applicable, Operators and persons acting on behalf of the OPFA must, before processing Personal Information, ensure that the records/facility housing the Personal Information will be kept secure and that appropriate measures and safeguards are in place to prevent any unauthorised access, disclosure and/or loss of such Personal Information.

7.2 Removing and downloading Personal Information on to portable devices from workplace equipment, or taking soft copies of Personal Information off-site, must be authorised in writing by the manager of the relevant department from where the information emanates, and a copy of such authorisation sent to the Information Officer. Removal of such information will be subject to the following provisions:

7.2.1. The person removing the Personal Information must explain and justify the operational need for the removal in relation to the volume and sensitivity of the Personal Information and ensure that the details of the Personal Information being removed is documented and recorded under a “removal register”;

7.2.2. The Personal Information to be removed must be strongly encrypted;

7.2.3. The person removing and using said data should only store the data necessary for their immediate needs and should remove the data as soon as possible once dealt with. Such removal should be confirmed by way of recordal in the removal register;

7.2.4. To avoid loss of encrypted data, or in case of failure of the encryption software, an unencrypted copy of the data must be held in a secure environment.

7.3 Where it is necessary to store Personal Information on portable devices such as laptops, USB flash drives, portable hard drives, CDs, DVDs, or any computer not owned by the OPFA, employees and where applicable, Operators and persons acting on behalf of the OPFA without exception must, before storing said Personal Information, ensure that the data is encrypted and is kept secure, and that appropriate measures and safeguards are in place to prevent unauthorised access, disclosure and loss of such Personal Information, and points 7.2.1- 7.2.4 will apply to this data.

7.4 Where paper or hard copies of Personal Information are removed from the OPFA premises, employees and where applicable, Operators and persons acting on behalf of the OPFA without exception must, before removing said Personal Information ensure that only that data necessary for the purpose it is being removed is taken, is documented in a removal register and is thereafter whilst away from the OPFA premises kept safe and secure, and that appropriate measures and safeguards are in place to prevent any unauthorised access, disclosure and loss of such Personal Information.

7.5 Paper or hard copies of Personal Information and portable electronic devices housing Personal Information should be stored in locked units and should not be left on desks overnight or in view of other employees or third parties.

7.6 Personal Information, which is no longer required, should be securely archived and retained, as per the OPFA Physical and Electronic Record Management Policy.

7.7 Personal Information must not be disclosed unlawfully to any third party.

7.8 Where an OPERATOR is to process Personal Information on behalf of the OPFA, such processing will be subject to a written OPERATOR agreement concluded between the OPFA and the OPERATOR, which agreement is to be substantially in same format as the standard OPFA OPERATOR agreement.

7.9 All losses of Personal Information must be reported, as soon as possible, to the relevant manager of the department from where the information emanates, and the Information Officer/Deputy Information Officer.

7.10 Negligent loss or unauthorised disclosure of Personal Information, or failure to report such events, may be treated as a disciplinary matter.

7.11 The OPFA via its Information Security Officer and IT department will continuously review its security controls and processes to ensure that all Personal Information is secure.

8. Access and Correction of Personal Information

8.1 In terms of POPIA, a Data Subject has the right to:

8.1.1 Request access to their Personal Information which the OPFA holds, if they follow the “Access to Information Procedure” set out under the OPFA PAIA Manual set out under the OPFA website;

8.1.2 Ask the OPFA to update, correct or delete any of its Personal Information, which the OPFA thereafter has a duty to correct, save where the OPFA is of the view

that the request is incorrect, invalid and / or unreasonable. The right to have personal information corrected or deleted shall apply to parties to a complaint during the course of an investigation but shall not apply once a determination is issued. Once a determination has been issued by the OPFA, the OPFA is legally obliged in terms of section 30L of the Pension Funds Act, 1956 to maintain a permanent record of the proceedings relating to the adjudication of a complaint and the evidence given. Should a party to a complaint request that their personal information is corrected after the issuing of a determination, such new personal information provided shall be separately attached to the record however the previous personal information provided will not be deleted;

8.1.3 Object to the OPFA processing their Personal Information, which the OPFA holds about them, by filing a notice of objection.

9. Information Officer

9.1 The OPFA has appointed an Information Officer and Deputy Information Officer who have been tasked with the primary responsibility for compliance with POPIA.

9.2 All the OPFA's employees are under a duty to:

9.2.1 Raise any concerns in respect of the processing of Personal Information with the Information Officer or Deputy Information Officer;

9.2.2 Promptly pass on to the Information Officer or Deputy Information Officer all Data Subject access requests and requests from third parties for Personal Information;

9.2.3 Report losses or unauthorised disclosures of Personal Information to the Information Officer or Deputy Information Officer as soon as such loss or disclosure has been noted; and

9.2.4 Address any queries or concerns about this Policy and/or compliance with POPIA with the Information officer or Deputy Information Officer.

10. Operators and Service Providers

Where any OPFA employee requires an OPFA service provider, contractor and/or agents (Operator) to process Personal Information for or on behalf of the OPFA, such employee shall ensure that prior to such processing a standard OPFA Operator Agreement is concluded with the Operator in respect of such processing.

11. General

Any transgression of this Policy will be investigated and may lead to disciplinary action being taken against the offender.

12. Version and Amendments

This Policy is effective as from 1 February 2021.

ANNEXURE A

Protection of Personal Information Act, 2013

Data Privacy Consent Notice

Declaration

This Data Privacy Consent Notice will apply to the OPFA ("Responsible Party")

On the one hand,

AND

The Responsible Party's EMPLOYEES, and/or ANY OTHER PERSON including without detracting from the generality thereof, any juristic or natural person, full time, fixed term, part time and temporary Responsible Party employees, prospective Responsible Party employees, employment candidates, bursary and study recipients, Responsible Party service providers, Responsible Party Operators, Responsible Party consumers and customers, parties to a complaint in terms of the Pension Funds Act, 1956, governmental, provincial and municipal agencies or entities, regulators, persons making enquiries and/or other third parties, including all associated, related and/or family members of such Data Subjects, or any person who may be acting on behalf of/or in a representative capacity in respect of the Data Subject, and- from whom the Responsible Party receives Personal Information, ("Data Subject"), on the other hand.

Table of Contents

1. Introduction

The Protection of Personal Information Act, 4 of 2013 ("POPIA"), regulates and controls the processing, including the collection, use, and transfer of a person's Personal Information.

In terms of POPIA, a person ("Responsible Party") has a legal duty to collect, use, transfer and destroy "(Process") another's ("Data Subject") Personal Information in a lawful, legitimate, and responsible manner and in accordance with the provisions and the eight processing conditions set out under POPIA.

Condition 1 – Accountability
Condition 2 – Processing limitation
Condition 3 – Purpose specification
Condition 4 – Further processing limitation
Condition 5 – Information quality
Condition 6 – Openness
Condition 7 – Security safeguards
Condition 8 – Data subject participation

Furthermore, unless the processing is-

a) necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is a party; or
b) required and complies with an obligation imposed by law on either the Data Subject or the Responsible Party; or
c) necessary to protect the legitimate interest(s) of the Data Subject or the Responsible Party; or
d) necessary for the proper performance of a public law duty by a public body; or
e) necessary for pursuing the Data Subject or the Responsible Party's legitimate interests, or that of a third party to whom the Personal Information is supplied,

all processing of a Data Subject's Personal Information must be done with the Data Subject's permission i.e. the Data Subject must consent to the processing of its Personal Information.

The Responsible Party does and will from time-to-time process Personal Information which belongs to or is held by a Data Subject.

Following this, to comply with POPIA, the Responsible Party requires the Data Subject's permission to process the Data Subject's Personal Information.

2. Explanatory Notes

This Data Privacy Consent Notice explains and sets out:

2.1 What Personal Information belonging to the Data Subject will be processed by the Responsible Party;

2.2 Why the Responsible Party needs the Data Subject's Personal Information;

2.3 What the Responsible Party will be do with the Data Subject's Personal Information;

2.4 Who the Responsible Party will share the Data Subject's Personal Information with;

2.5 What the Responsible Party will do with the Data Subject's Personal Information as and when the purpose for the processing comes to an end.

3. Application of this Data Privacy Consent Notice

This Data Privacy Consent Notice will apply to the Responsible Party, and to the Data Subject, and/or the Data Subject's Personal Information which is processed or may be processed by the Responsible Party, including any processing of the Data Subject's Personal Information by any Operators duly appointed by the Responsible Party.

4. Purpose for the Collection

For the Responsible Party to pursue its business objectives and strategies, the Responsible Party needs to process the Data Subject's or party to a complaint's Personal Information, which Personal Information will be used for several lawful purposes, including, inter alia, the following:

4.1 For the purposes of complying with a variety of lawful obligations, including without detracting from the generality thereof:

- Administrative laws
- Responsible Party laws
- Corporate governance codes
- Communication laws
- Customs and Excise laws
- Environmental laws
- Financial and Tax laws
- Health and Safety laws
- Labour and Employment laws
- Medical Aid laws
- Pension/Retirement fund laws

- Public finance laws

4.2 For the purposes of conducting investigations and issuing determinations in terms of the Pension Funds Act, 1956 and all matters incidental thereto including but not limited to applications for reconsideration before the Financial Services Tribunal in terms of the Financial Sector Regulation Act, 2017.

4.3 For the purposes of carrying out actions for the conclusion and performance of a contract between the Responsible Party and the Data Subject;

4.4 For the purposes of protecting the Data Subject's and/or the Responsible Party's legitimate interest(s), including the performance of risk assessments and risk profiles;

4.5 Where required by law or Responsible Party policy receiving from or providing to any credit bureau or credit provider or credit association information about the Data Subject's credit record, including Personal Information about any judgement or default history;

4.6 For the purposes of any proposed or actual merger, acquisition, or any form of sale of some or all the Responsible Party's assets, providing the Data Subject's Personal Information to third parties, in connection with the evaluation of the transaction and related due diligence procedures;

4.7 For the purposes of contacting the Data Subject and attending to the Data Subject's enquiries and requests;

4.8 For the purposes of providing the Data Subject from time to time with information regarding the Responsible Party, its directors, employees, services and goods and other ad hoc business-related information. Should the Data Subject not want to receive these specific communications please specifically decline the opportunity by contacting us with your request.

4.9 For academic research and statistical analysis purposes, including data analysis, testing, research and product development and product review purposes;

4.10 For the purposes of a pursuing the Data Subject's and/or the Responsible Party's legitimate interests, or that of a third party to whom the Personal Information is supplied;

4.11 For the purposes of providing, maintaining, and improving the Responsible Party's products and services, and to monitor and analyse various usage and activity trends regarding thereto;

4.12 For the purposes of performing internal operations, including management of employees, employee wellness programmes, the performance of all required HR and IR functions, call centres, customer care lines and enquiries, attending to all financial matters including budgeting, planning, invoicing, facilitating, and making payments, making deliveries, sending receipts, and generally providing commercial support, where needed, requested, or required;

4.13 For the purposes of preventing fraud and abuse of the Responsible Party's processes, systems, procedures, and operations, including conducting internal and external investigations and disciplinary enquiries and hearings.

The Data Subject and/or the parties to a complaint agrees that the Responsible Party may use all the Personal Information which the Data Subject provides to the Responsible Party, which the responsible Party requires for the purposes of pursuing its objectives and strategies.

The Responsible Party in turn undertakes that it will only use the Data Subject's or parties to a complaint's Personal Information for the purposes mentioned above and for no other reason, unless with the Data Subject's or parties to a complaint's prior authorisation.

5. Consequences of the Data Subject withholding Consent or Personal Information

Should the Data Subject refuse to provide the Responsible Party with his/her/its Personal Information, which is required by the Responsible Party for the purposes indicated above, and the required consent to process the Personal Information, then the Responsible Party will be unable to engage with the Data Subject or enter into any agreement or relationship with the Data Subject.

Should any of the parties to a complaint refuse to provide the Responsible Party with his/her/its Personal Information, which is required by the Responsible Party for purposes mentioned in 4.2 above, then the Responsible Party may in its own discretion dispose of a complaint in the absence of such information.

6. Storage, Retention and Destruction of Information

Personal Information will be stored electronically in a centralised database, which, for operational reasons, will be accessible to all within the Responsible Party on a need to know and business basis, save that where appropriate, some Personal Information may be retained in hard copy.

All Personal Information will be held and/or stored securely. In this regard the Responsible Party undertakes to conduct regular audits in respect of the safety and the security of Personal Information.

As and when Personal Information is no longer required, since the purpose for which the Personal Information was held has come to an end and expired, such Personal Information

will be safely and securely archived for a period of 7 years, as per the requirements of the Companies Act, 71 of 2008, or longer should this be required by any other law applicable in South Africa including section 30L of the Pension Funds Act,1956. The Responsible Party thereafter will ensure that such Personal Information is permanently destroyed.

7. Access by Others and Cross Border Transfer

The Responsible Party may from time to time have to disclose Personal Information to other parties, including regulators and/or governmental officials, international service providers and related companies or agents, but such disclosure will always be subject to an agreement, which will be concluded between the Responsible Party and the party to whom it is disclosing Personal Information, which contractually obliges the recipient of the Personal Information to comply with strict confidentiality and data security conditions, unless excluded by POPIA and/or other relevant legislation.

Where Personal Information and related data is transferred to a country which is situated outside the borders of South Africa, the Personal Information will only be transferred to those countries which have similar data privacy laws in place, or where the recipient of the Personal Information is bound contractually to a no lesser set of obligations than those imposed by POPIA.

8. Right to Object and Complaints

The Data Subjects or parties to a complaint are encouraged to make immediate contact with the Responsible Party Information Officer at any time if he/she/it is not comfortable or satisfied with the way the Responsible Party is processing Personal Information.
On receipt of the objection, the Responsible Party will place a hold on any further processing until the cause of the objection has been resolved. If the Data Subject is not satisfied with such process, the Data Subject has the right to lodge a complaint with the Information Regulator.

9. Accuracy of Information and Onus

POPIA requires that all the Data Subject's Personal Information and related details as supplied, are complete, accurate and up to date. While the Responsible Party will always use its best endeavours to ensure that the Data Subject's and parties to a complaint's Personal Information is reliable, it will be the Data Subject's or parties to a complaint's responsibility to advise the Responsible Party of any changes to the Personal Information, as and when these may occur.

10. Access to Information by the Data Subject

The Data Subject or party to a complaint has the right at any time to request the Responsible Party to provide details of his/her/its Personal Information which the Responsible Party holds and/or the purpose for which it has been used provided that such request is made using the Responsible Party's PAIA process, which procedure can be accessed by downloading and completing the standard request for information form, kept in the Responsible Party's PAIA Manual, which can be found on the Responsible Party's website.

11. Amendments and Binding on Successors in Title

The Responsible Party reserves the right to amend this Data Privacy Consent Notice from time to time.

The rights and obligations of the parties under this Data Privacy Consent Notice will be binding on, and will be of the benefit to, each of the parties' successors in title and/or assigns where applicable.

12. Declaration and Data Privacy Consent

The Data Subject or party to a complaint confirms that the Personal Information provided is accurate, up to date, not misleading and is complete in all respects, save where same may change and then, in such an event, the Data Subject or party to a complaint undertakes to advise the Responsible Party or its Operator(s) of these changes.

The Data Subject or party to a complaint, in providing the required Personal Information to the Responsible Party and/or to its Operator(s), consents and gives the Responsible Party permission to process and further process the Personal Information as and where required and acknowledges that the Data Subject or party to a complaint understands the purposes for which the Personal Information is required, and for what it will be used.

Should any of the Personal Information which has been provided concern a legal entity, the Data Subject or party to a complaint confirms that he/she has the necessary authority to act on behalf of such legal entity, and that he/she has the right to provide the Personal Information and/or the required consent to use said Personal Information, on behalf of the legal entity.

Should any of the Personal Information belong to any of the Data Subject's or party to a complaint's dependants and/or beneficiaries who are under 18 years old, the Data Subject or

party to a complaint, in his/her capacity as their legal guardian and competent person, gives the Responsible Party authorisation to process their Personal Information for the purposes for which these details were given.

For further information contact:

OPFA's Deputy Information Officer: nondumiso.ntshangase@pfa.org.za