PRIVACY POLICY

Protection Of Private Information (POPIA) Policy

pns group

In-store Impact. Delivered

Table of Contents

1. Introduction

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA").

POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

Through the provision of quality goods and services, PNS Group is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.

A person's right to privacy entails having control over their personal information and being able to conduct their affairs relatively free from unwanted intrusions.

Given the importance of privacy, PNS Group is committed to effectively managing personal information in accordance with POPIA's provisions.

2. Definitions

2.1 Personal Information

Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

- Race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language, and birth of a person;
- Information relating to the education or the medical, financial, criminal or employment history of the person;
- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person;
- The biometric information of the person;
- The personal 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.

2.2 Data Subject

This refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies the organisation with products or other goods.

2.3 Responsible Party

The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the organisation is the responsible party.

2.4 Operator

An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, a third-party service provider that has contracted with the organisation to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

2.5 Information Officer

The Information Officer is responsible for ensuring the organisation's compliance with POPIA. Where no Information Officer is appointed, the head of the organisation will be responsible for performing the Information Officer's duties.

Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

2.6 Processing

The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

- 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 any restriction, degradation, erasure, or destruction of information.

2.7 Record

Means any recorded information, regardless of form or medium, including:

- 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.

2.8 Filing System

Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.9 Unique Identifier

Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

2.10 Deidentify

This means to delete any information that identifies a data subject, or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

2.11 Reidentify

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.12 Consent

Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

2.13 Direct Marketing

Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
- Requesting the data subject to make a donation of any kind for any reason;

2.14 Biometrics

Means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning, facial recognition and voice recognition.

3. Purpose

This purpose of this policy is to protect PNS GROUP from the compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality. For instance, PnS GROUP could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose PnS GROUP uses information relating to them.
- Reputational damage. For instance, the organisation could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by PnS GROUP

This policy demonstrates PnS GROUP 's commitment to protecting the privacy rights of data subjects in the following manner:

- Through stating desired behavior and directing compliance with the provisions of POPIA and best practice.
- By cultivating an organisational culture that recognises privacy as a valuable human right.
- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.

- By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of PnS GROUP
- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers to protect the interests of PnS GROUP and data subjects.
- By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4. Organisational Scope

This policy and its guiding principles apply to:

- PNS GROUP 's governing body
- All branches, business units and divisions of PNS GROUP
- All employees
- All contractors, suppliers and other persons acting on behalf of PNS GROUP

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the organisation's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with POPIA's provisions is activated in any situation where there is:

- A processing of personal information entered into a record by or for a responsible person who is domiciled in South Africa.

  POPIA does not apply in situations where the processing of personal information:

- Is concluded in the course of purely personal or household activities, or
- Where the personal information has been de-identified.

5. Rights of Data Subjects

Where appropriate, PnS GROUP will ensure that its employees, customers and suppliers are made aware of the rights conferred upon them as data subjects. PnS GROUP will ensure that it gives effect to the following rights:

5.1 The right to access Personal Information

PnS GROUP recognises that a data subject has the right to establish whether PNS GROUP holds personal information related to them or it including the right to request access to that personal information. An example of a "Personal Information Request Form" can be found under Annexure A.

5.2 The right to have Personal Information corrected or deleted

The data subject has the right to request, where necessary, that their or its personal information must be corrected or deleted when PNS GROUP is no longer authorised to retain the personal information.

5.3 The right to object to the processing of Personal Information

The data subject has the right, on reasonable grounds, to object to the processing of their or its personal information.

In such circumstances, PnS GROUP will give due consideration to the request and the requirements of POPIA. PnS GROUP may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

5.4 The right to complain to the Information Regulator

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of their or its personal information.

An example of a "POPI Complaint Form" can be found under Annexure B.

5.5 The right to be informed

The data subject has the right to be notified that their or its personal information is being collected by PnS GROUP. The data subject also has the right to be notified in any situation where PnS GROUP has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

PnS GROUP may possess records relating to suppliers, shareholders, contractors service providers, employees and customers as follows:

Entity Type	Personal Information Processed
Customers: Natural Persons	Names; contact details; physical and postal addresses; date of birth; ID number; tax related information; nationality; gender; confidential correspondence
Customer – Juristic Persons / Entities	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information
Contracted Service Providers	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information
Employees / Directors	Gender; pregnancy; marital status; colour, race; age; language; education information; financial information; employment history; ID number; physical and postal address; contact details; opinions; criminal record; well-being

Subjects of categories of records of personal information held under the care of PNS GROUP:

- Attendance registers
- Correspondence
- Founding Documents
- Licences (categories)
- Minutes of Management Meetings
- Minutes of Staff Meetings
- Shareholder Register
- Statutory Returns
- Conditions of Service
- Employee Records
- Employment Contracts
- Employment Equity Records
- General Correspondence
- Industrial and Labour Relations Records
- Information relating to Health and Safety Regulations
- Pension and Provident Fund Records
- Performance Appraisals
- Personnel Guidelines, Policies and Procedures
- Remuneration Records and Policies
- Salary Surveys
- Skills Requirements
- Staff Recruitment Policies
- Statutory Records
- Training Records
- Brochures on Company Information
- Client and Customer Registry
- Contracts
- Information relating to Employee Sales Performance
- Information relating to Work-In-Progress
- Marketing and Future Strategies
- Marketing Records
- Production Records
- Sales Records
- Suppliers Registry
- Annual Financial Statements
- Asset Register
- Banking Records
- Budgets
- Financial Transactions

- Insurance Information
- Internal Audit Records
- Management Accounts
- Purchase and Order Information
- Stock Records
- Tax Records (company and employee)
- IT Policies and Procedures
- Network Diagrams
- User Manuals

Subjects of categories of personal records held under the care of PNS GROUP:

- FICA Docs
- Identity Numbers
- Dates of birth
- Telephone numbers
- eMails
- Addresses
- Banking details
- Bank account numbers
- Licence numbers
- Registration numbers
- BEE Certificates
- Contractual agreements
- Tender documents
- Invoices

Customer personal information shared by PNS GROUP

- Telephone numbers
- Emails
- Addresses
- Registration numbers
- BEE Certificates
- Contractual agreements
- Tender documents
- Invoices

Employee information received by PnS GROUP

- Provident/pension funds
- Medical aid funds

ICT practices carried out by PnS GROUP

- Physical security, (PC's locked to fixture/locked computer room)
- Network security controls
- Password controls
- Virus & Malware protection
- Software updates
- Disaster recovery & back-up policy

Transfer of personal information outside of the Republic of South Africa

Personal Information may be stored in data servers hosted outside South Africa, which may not have adequate data protection laws. The PNS GROUP will endeavour to ensure that the companies we deal with through our retail channels will make all reasonable efforts to secure said data and Personal Information.

6. General Guiding Principles

All employees and persons acting on behalf of PnS GROUP will at all times be subject to, and act in accordance with, the following guiding principles:

6.1 Accountability

Failing to comply with POPIA could potentially damage PnS GROUP 's reputation or expose the organisation to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

PnS GROUP will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, PnS GROUP will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

6.2 Processing limitation

PnS GROUP will ensure that personal information under its control is processed:

- in a fair, lawful, and non-excessive manner, and
- only with the informed consent of the data subject, and
- only for a specifically defined purpose.

PnS GROUP will inform the data subject of the reasons for collecting their or its personal information and obtain written consent prior to processing personal information.

Alternatively, where services or transactions are concluded over the telephone or electronic video feed, PnS GROUP will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.

PnS GROUP will under no circumstances distribute or share personal information between separate legal entities, associated organisations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

Where applicable, the data subject must be informed of the possibility that their or it's personal information will be shared with other aspects of the organisation's business and be provided with the reasons for doing so.

An example of a "POPI Notice and Consent Form" can be found under Annexure C.

6.3 Purpose specification

All of PnS GROUP 's business units and operations must be informed by the principle of transparency. PnS GROUP will process personal information only for specific, explicitly defined and legitimate reasons.

PnS GROUP will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

6.4 Further processing limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Therefore, where PnS GROUP seeks to process personal information it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, PnS GROUP will first obtain additional consent from the data subject.

6.5 Information quality

PnS GROUP will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

The more important it is that the personal information be accurate, the greater the effort the organisation will put into ensuring its accuracy.

Where personal information is collected or received from third parties, PnS GROUP will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

6.6 Open communication

PmS GROUP will take reasonable steps to ensure that data subjects are notified (are at all times aware) that their or its personal information is being collected including the purpose for which it is being collected and processed.

PNS GROUP will ensure that it establishes and maintains a "contact us" facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:

- Enquire whether the organisation holds related personal information, or
- Request access to related personal information, or
- Request the organisation to update or correct related personal information, or
- Make a complaint concerning the processing of personal information.

6.6 Security safeguards

PnS GROUP will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.

PnS GROUP will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the organisation's IT network.

PnS GROUP will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the organisation is responsible.

All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

PnS GROUP 's operators and third-party service providers will be required to enter into service level agreements with the organisation where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement. An example of "Employee Consent and Confidentiality Clause" for inclusion in PNS GROUP 's employment contracts can be found under Annexure D. An example of an "SLA Confidentiality Clause" for inclusion in PNS GROUP 's service level agreements can be found under Annexure E.

6.7 Data Subject participation

A data subject may request the correction or deletion of their or its personal information held by the organisation. PnS GROUP will ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information. Where applicable, the organisation will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7. Information Officers

PnS GROUP will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer. PNS GROUP 's Information Officer is responsible for ensuring compliance with POPIA.

There are no legal requirements under POPIA for PnS GROUP to appoint an Information Officer. Appointing an Information Officer is however, considered to be a good business practice, particularly within larger organisations.

Where no Information Officer is appointed, the head of PnS GROUP will assume the role of the Information Officer. Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers.

Once appointed, PnS GROUP will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties. An example of an "Information Officer Appointment Letter" can be found under Annexure F.

8. Specific Duties and Responsibilities

8.1 Governing Body

PnS GROUP ‘s governing body cannot delegate its accountability and is ultimately answerable for ensuring that the organisation meets its legal obligations in terms of POPIA. The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The governing body is responsible for ensuring that:

- PNS GROUP appoints an Information Officer, and where necessary, a Deputy Information Officer.
- All persons responsible for the processing of personal information on behalf of the organisation:
  - are appropriately trained and supervised to do so,
  - understand that they are contractually obligated to protect the personal information they come into contact with, and
  - are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
- Data subjects who want to make enquiries about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
- The scheduling of a periodic POPIA Audit to accurately assess and review the ways in which PnS GROUP collects, holds, uses, shares, discloses, destroys, and processes personal information.
- Ensuring that employees and other persons acting on behalf of PnS GROUP are fully aware of the risks associated with the processing of personal information and that they remain informed about PnS GROUP 's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of PnS GROUP.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by PnS GROUP 's data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

The Deputy Information Officer will assist the Information Officer in performing their duties.

8.2 Chief Information Officer

PnS GROUP 's Chief Information Officer is responsible for:

- Ensuring that PNS GROUP 's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
- Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion, and malicious hacking attempts.

- Ensuring that personal information being transferred electronically is encrypted.
- Ensuring that all serves and computers containing personal information are protected by a firewall and the latest security software.
- Performing regular IT audits to ensure that the security of the organisation 's hardware and software systems are functioning properly.
- Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
- Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the organisation's behalf. For instance, cloud computing services.

8.3 General Manager: Marketing

PnS GROUP ‘s General Manager: Marketing is responsible for:

- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the organisation's website, including those attached to communications such as emails and electronic newsletters.
- Addressing any personal information protection queries from journalists or media outlets such as newspapers.
- Where necessary, working with persons acting on behalf of the organisation to ensure that any outsourced marketing initiatives comply with POPIA.

8.4 Employees and other persons acting on behalf of PnS GROUP

- Employees and other persons acting on behalf of PNS GROUP will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.
- Employees and other persons acting on behalf of PnS GROUP are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.
- Employees and other persons acting on behalf of PnS GROUP may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within PnS GROUP or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties.
- Employees and other persons acting on behalf of PnS GROUP must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.
- Employees and other persons acting on behalf of PnS GROUP will only process personal information where:
- The data subject, consents to the processing; or
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- The processing complies with an obligation imposed by law on the responsible party; or
- The processing protects a legitimate interest of the data subject; or
- The processing is necessary for pursuing the legitimate interests of the organisation or of a third party to whom the information is supplied.
- Furthermore, personal information will only be processed where the data subject:

- Clearly understands why and for what purpose their or its personal information is being collected; and
- Has granted the organisation with explicit written or verbally recorded consent to process their or its personal information.
- Employees and other persons acting on behalf of PnS GROUP will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.
- Informed consent is therefore when the data subject clearly understands for what purpose their or its personal information is needed and who it will be shared with. Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, PnS GROUP will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.
- Consent to process a data subject's personal information will be obtained directly from the data subject, except where:
- The personal information has been made public, or
- Where valid consent has been given to a third party, or
- The information is necessary for effective law enforcement.
- Employees and other persons acting on behalf of PnS GROUP will under no circumstances:
- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the organisation's central database or a dedicated server.
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
- Transfer personal information outside of South Africa without the express permission from the Information Officer.
- Employees and other persons acting on behalf of PnS GROUP are responsible for:
- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the organisation, with the sending or sharing of personal information to or with authorised external persons.
- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- Ensuring that where personal information is stored on removable storage medias such as external drives, CDs, or DVDs that these are kept locked away securely when not being used.
- Ensuring that where personal information is stored on paper, that such hard copy records are

kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.

- Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
- Undergoing POPIA Awareness training from time to time.
- Where an employee, or a person acting on behalf of PnS GROUP, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, they must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

9. POPIA Audit

PnS GROUP 's Information Officer will schedule periodic POPIA Audits. The purpose of a POPIA audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy personal information.
- Determine the flow of personal information throughout PnS GROUP. For instance, PnS GROUP 's various business units, divisions, branches and other associated organisations.
- Redefine the purpose for gathering and processing personal information.
- Ensure that the processing parameters are still adequately limited.
- Ensure that new data subjects are made aware of the processing of their personal information.
- Re-establish the rationale for any further processing where information is received via a third party.
- Verify the quality and security of personal information.
- Monitor the extend of compliance with POPIA and this policy.
- Monitor the effectiveness of internal controls established to manage the organisation's POPI related compliance risk.

In performing the POPIA Audit, Information Officers will liaise with line managers in order to identify areas within in PnS GROUP 's operation that are most vulnerable or susceptible to the unlawful processing of personal information. Information Officers will be permitted direct access to and have demonstrable support from line managers and the organisation's governing body in performing their duties.

10. Request to Access Personal Information

Data subjects have the right to:

- Request what personal information the organisation holds about them and why.
- Request access to their personal information.

- Be informed how to keep their personal information up to date.

Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a "Personal Information Request Form".

Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against the organisation's PAIA Manual. The Information Officer will process all requests within a reasonable time.

11. POPIA Complaints Procedure

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. PNS GROUP takes all complaints very seriously and will address all POPIA related complaints in accordance with the following procedure:

- POPIA complaints must be submitted to the organisation in writing. Where so required, the Information Officer will provide the data subject with a "POPIA Complaint Form".
- Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
- The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavor to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the organisation's data subjects.
- Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with the organisation's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.
- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the organisation's governing body within 7 working days of receipt of the complaint. In all instances, the organisation will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
- The Information Officer's response to the data subject may comprise any of the following:
  - A suggested remedy for the complaint,
  - A dismissal of the complaint and the reasons as to why it was dismissed,
  - An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
- The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where required. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPIA related complaints.

12. Disciplinary Action

Where a POPIA complaint or a POPIA infringement investigation has been finalised, PNS GROUP may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

In the case of ignorance or minor negligence, PNS GROUP will undertake to provide further awareness training to the employee.

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which PNS GROUP may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

Examples of immediate actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action.
- A referral to appropriate law enforcement agencies for criminal investigation.
- Recovery of funds and assets in order to limit any prejudice or damages caused.

13. Regulatory and Legislative Management

PnS GROUP manages regulations and legislation within its defined Cyber Security Compliance Policy Framework and the Data Protection Retention and Disposal Policy. Other Statutory records held by PnS GROUP are;

Specific Acts

- Promotion of Access to Information Act, No 2 of 2000 (“PAIA”)
- Protection of Personal Information Act, No 4 of 2013 (“POPIA”)
- Electronic Communications and Transactions Act 25 of 2002
- Regulations Relating to The Protection of Personal Information, No. R. 1383, 2018

Other Acts

- Basic Conditions of Employment 75 of 1997
- Companies Act 71 of 2008
- Employment Equity Act 55 of 1998
- Income Tax Act 95 of 1967
- Labour Relations Act 66 of 1995
- Occupational Health and Safety Act 85 of 1993
- Skills Development Act 97 of 1998
- Skills Development Levies Act 9 of 1999
- Unemployment Contributions Act 4 of 2002
- Unemployment Insurance Act 63 of 2001
- Value Added Tax Act 89 of 1991

14. References

- All policies and procedures are maintained by the Chief Information Officer. These include:
- The Risk Register Incorporating compliance
- All documented Policies, Processes and Procedures
- Requests for information or documentation to be submitted to popia@pns.co.za

15. Approval Structure

Approval required by Board of Directors and Executive Management.

16. Policy Sponsor

The Chief Information Officer

17. Contact Person

The following person may be contacted in relation to this policy:

Ruan Lombard: Chief Information Officer

18. Reference Documents

System Development and Maintenance
Software Asset Control Policy

Disaster Recovery and Risk Management
Disaster Recovery Policy
Media Handling Policy
Risk Management Policy

Network Security and Access Control
Logical Access Control Policy
Remote Access Policy
Network and wireless security policy

Computer Installations and Operations
Antivirus and Malware Policy
Change and Release Management Policy
Hardware Asset Policy
Physical and Environmental Protection Policy
Vulnerability and Patch Management Policy
Security Incident Management Policy
Systems Monitoring Policy

Employee Security
Acceptable Use Policy

Company Device Policy
Email and Internet Usage Policy
Information Security Policy
ICT Policy Framework

Information Asset Management

Information Exchange Policy
Data Protection Retention and Disposal Policy

ANNEXURE A:

PERSONAL INFORMATION REQUEST FORM

PERSONAL INFORMATION REQUEST FORM

pns group
In-store Impact. Delivered

PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer: _____ In terms of (Section 18(1) of the Promotion of Access to Information Act, 2000) (Act No. 2 of 2000) [Regulation 6]	
Name:	Ruan Lombard
Contact Number:	+27 12 460 3331
Email Address:	popia@pns.co.za
Please be aware that we may require you to provide proof of identification prior to processing your request.	
Section A. Particulars of Data Subject	
Name & Surname:	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	
Section B. Request	
Method of Access Preferred: Paper copies of the documents ☐ Electronic copies of the documents ☐	
I request the organisation to: (Please tick applicable box) Inform me whether it holds any of my personal information. ☐ Provide me with a record or description of my personal information. ☐ Correct or update my personal information. ☐ Destroy or delete a record of my personal information ☐	
Please complete below any further information on the documents you are requesting (Reference numbers, further particulars etc,	
Section C. Signature	
Signature: **Date:**	

ANNEXURE B:

POPIA COMPLAINT FORM

POPIA COMPLAINT FORM

pns group
In-store Impact. Delivered

COMPLAINT REGARDING THE PROTECTION OF PERSONAL INFORMATION

Please submit the completed form to the Information Officer: _____ In terms of (Section 74) of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013)			
Name:	Ruan Lombard		
Contact Number:	+27 12 460 3331		
Email Address:	popia@pns.co.za		
NOTE: Where we are unable to resolve your complaint to your satisfaction you have the right to complain take up your complaint with the Information Regulator: Complaints.IR@justice.gov.za **– 33 Hoofd Street, Forum III, 3rd Floor, Braampark**			
Section A. Particulars of Complainant (Please provide proof Identification along with the complaint form)			
First Name:		**Surname:**	
Identity Number:		**Postal Address:**	
Contact Number:		**Email Address:**	
Section B. Details of Complaint			
Section B. Desired Outcome			
Section C. Signature			
Signature: **Date:**			

ANNEXURE C:
POPIA NOTICE AND CONSENT FORM

POPIA NOTICE AND CONSENT FORM

pns group
In-store Impact. Delivered

CONSENT TO PROCESS PERSONAL INFORMATION

Please submit the completed form to the Information Officer: _____
In terms of (Section 18) of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013)

Name:	Ruan Lombard
Contact Number:	+27 12 460 3331
Email Address:	popia@pns.co.za

Section A. Purpose for Collection and Processing the Information

The purpose for the collection of your Personal Information and the reason for the Company requiring your Personal Information is to enable the Company:

i. to comply with lawful obligations, including amongst others, all applicable labour, tax and financial legislation such as:
   - The Financial Advisory and Intermediary Services Act 37 of 2002 (FAIS)
   - The Financial Intelligence Centre Act 38 of 2001 (FICA)
   - The National Credit Act 34 of 2005
   - The Broad Based Black Economic Empowerment laws (B-BBEE)

ii. to give effect to a contractual relationship between the Company and yourself;
iii. to conduct its business operations; and
iv. to protect the legitimate interests of the Company, yourself and or any third parties.

All Personal Information which you provide to the Company will only be used for the purposes set out above.

Section B. Declaration and Informed Consent

I consent to providing the Personal Information required, to the Company, on the understanding that the Company is responsible to abide by the principles set out in POPIA, in the Company POPIA Policy, and in this document.

I declare that all Personal Information being supplied by me to the Company is accurate, up to date, not misleading, and that it is complete in all material respects.

I undertake to advise the Company immediately of any changes to my Personal Information, should any of the details change.

By providing the Company with my Personal Information, I consent and give the Company permission to process and further process the Personal Information, as and when required, that I supply to the Company, understanding the purposes for which the Personal Information is required and for which it will be use.

First Name and Surname:

Signature:

Date:

ANNEXURE D:
EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

- "Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal 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 whether the information is recorded electronically or otherwise.
- "POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.
- The employer undertakes to process the PI of the employee only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the employer's relevant policy available to the employee on request and only to the extent that it is necessary to discharge its obligations and to perform its functions as an employer and within the framework of the employment relationship and as required by South African law.
- The employee acknowledges that the collection of their PI is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the employer. The employee therefore irrevocably and unconditionally agrees:
    - That they are notified of the purpose and reason for the collection and processing of their PI insofar as it relates to the employer's discharge of its obligations and to perform its functions as an employer.
    - That they consent and authorises the employer to undertake the collection, processing, and further processing of the employee's PI by the employer for the purposes of securing and further facilitating the employee's employment with the employer.
    - Without deviating from the afore stated, the employee consents to the employer's collection and processing of PI pursuant to any of the employer's Internet, Email, and Interception policies in place insofar as PI of the employee is contained in relevant electronic communications.
        - To make available to the employer all necessary PI required by the employer for the purpose of securing and further facilitating the employee's employment with the employer.
        - To absolve the employer from any liability in terms of. POPIA for failing to obtain the employee's consent or to notify the employee of the reason for the processing of any of the employee's PI.

To the disclosure of their PI by the employer to any third party, where the employer has a legal or contractual duty to disclose such PI.

- The employee further agrees to the disclosure their PI for any reason enabling the employer to carry out or to comply with any business obligation the employer may have or to pursue a legitimate interest of the employer in order for the employer to perform its business on a day-to-day basis.
- The employee authorises the employer to transfer their PI outside of the Republic of South Africa for any legitimate business purpose of the employer within the international community. The employer undertakes

not to transfer or disclose their PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.

- The employee acknowledges that during the performance of their services they may gain access to and become acquainted with the personal information of certain clients, suppliers, and other employees. The employee will treat personal information as a confidential business asset and agrees to respect the privacy of clients, suppliers, and other employees.
- To the extent that they exposed to or insofar as PI of other employees or third parties are disclosed to them, the employee hereby agrees to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or employees .
- Employees may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the organisation or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform their duties on behalf of the employer.

ANNEXURE E:
SLA CONFIDENTIALITY CLAUSE

SLA Confidentiality Clause

- Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal 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 whether the information is recorded electronically or otherwise.
- "POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.
- The parties acknowledge that for the purposes of this agreement that the parties may come into contact with or have access to PI and other information that may be classified or deemed as private or confidential and for which the other party is responsible. Such PI may also be deemed or considered as private and confidential as ii relates to any third party who may be directly or indirectly associated with this agreement. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value.
- The parties agree that they will at all times comply with POPIA's Regulations and Codes of Conduct and that they shall only collect, use, and process PI they come into contact with pursuant to this agreement in a lawful manner, and only to the extent required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.
- The parties agree that it shall put in place, and at all times maintain, appropriate physical, technological, and contractual security measures to ensure the protection and confidentiality of PI that they, or its employees, its contractors or other authorised individuals comes into contact with pursuant to this agreement.
- Unless so required by law, the parties agree that it shall not disclose any PI as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any PI out of the Republic of South Africa.

ANNEXURE F:
INFORMATION OFFICER APPOINTMENT LETTER

- I herewith and with immediate effect appoint you as the Information Officer as required by the Protection of Personal Information Act (Act 4 of 2013). This appointment may at any time be withdrawn or amended in writing.
- You are entrusted with the following responsibilities:
- Taking steps to ensure the organisation's reasonable compliance with the provision of POPIA.
- Keeping the governing body updated about the organisation's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with the organisation's personal information processing procedures.
- This will include reviewing the organisation's information protection procedures and related policies.
- Ensuring that POPI Audits are scheduled and conducted on a regular basis.
- Ensuring that the organisation makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the organisation, to do so. For instance, maintaining a "contact us" facility on the organisation's website.
- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include overseeing the amendment of the organisation's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about the organisation's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the organisation.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by the organisation's data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.