PGCO
Accounting | Tax | Advisory
www.pgco.co.za

PGCO Advisory Incorporated

Johannesburg: 1st Floor | 155 West Street | Sandton | 2196 | South Africa
Durban: 7 Menston Road | Westville | Durban | 3629 | South Africa

+27 11 568 0755 info@pgco.co.za pgco.co.za

PROTECTION OF PERSONAL INFORMATION POLICY

POPIA POLICY

EFFECTIVE FROM 1ST JULY 2026

BACKGROUND TO DATA PRIVACY IN SOUTH AFRICA

The Protection of Personal Information Act, 4 of 2013, ("POPIA"), which came into force on 1 July 2021, is a statute that regulates the use and processing of a person and/or legal entity's personal information, in order to protect and give effect to a person and/or legal entity's rights to privacy, including the right not to have their personal information misused, abused or used for ulterior purposes.

POPIA applies to personal information that is the property of individuals and legal entities ("Data Subjects") that is processed, be it in an automated or non-automated manner in South Africa, by another ("Responsible Party") and places a duty to use it lawfully and only for a specific and defined purpose(s) on any Responsible Party who is processing a Data Subject's personal information.

In terms of POPIA, PGCO Advisory Incorporated ("The Company"), as a Responsible Party, is required to appoint an Information Officer ("IO") and Deputy Information Officers ("DIOs"), to be responsible for establishing a POPIA Compliance Framework, and who is following this, are required to assess, analyze and understand what types of personal information the Company is processing which belongs to Data Subjects and to thereafter develop certain processes and procedures, including a POPIA Policy, which have to be followed by all Company personnel when they process and use the personal information of third parties.

The Company, during the course of its business activities, does and will continue to collect, store and process personal information about the Company employees, its customers, suppliers and other third parties.

Furthermore, the Company processes different types of personal information including names, addresses, Identity Numbers, phone numbers and the like which pertain to current, past and prospective employees and customers, suppliers, and others who the Company communicates and deals with, and which processing is carried out for a variety of purposes, including for business, compliance and legal purposes.

The Company also processes special personal information including gender, sex, marital status, race and the like for the purposes of recruitment, employment equity reporting, legal compliance and for the facilitation of union fees and memberships.

The Company is confident that whilst this personal information is held on paper or on a computer or other media, such storage is subject to the prescribed legal safeguards as specified in POPIA and other regulations.

This Policy, which applies to PGCO Advisory Incorporated, sets out how all personnel at PGCO Advisory Incorporated (hereinafter referred to collectively as the "Company") are to conduct the processing of and use of third-party information, which information needs to be processed lawfully and in accordance with POPIA.

PGCO
Accounting I Tax I Advisory
www.pgco.co.za

Contents

1. STATEMENT FROM THE COMPANY'S FOUNDER

1.1 The Company has been conducting business with the highest level of integrity, honour and respect, in accordance with the highest ethical standards and in full compliance with all applicable laws, including the statute known as the Protection of Personal Information Act, 4 of 2013, (POPIA), which regulates the Processing of Personal Information.

1.2 The Protection of Personal Information Policy has been developed for PGCO Advisory Incorporated in order to provide clear guidance to all employees and any persons who Process Personal Information on behalf of the Company in regard to how they are to Process Personal Information, thereby ensuring that all Personal Information Processed by the Company is done in a lawful, transparent and consistent manner and in full compliance with all and any applicable data protection laws which may from time to time apply to its operations.

1.3 The Company requires compliance with all its policies, including this Protection of Personal Information Policy.

2. INFORMATION PROCESSING TERMS AND DEFINITIONS

POPIA makes use of certain terms and references that will be used in this Policy, which are explained below:

2.1. "Company" means PGCO Advisory Incorporated, a Personal Liability Company in South Africa with registration number 2020/127315/21 and its primary location of 1st Floor, 155 West St, Sandton, 2196 and 2 North Road, Duxberry, Sandton, 2191.

2.2. "Consent" means in relation to POPIA, any freely given, specific, informed and unambiguous

indication of the Data Subject's wishes by which they, by a statement or by a clear positive

action, signify agreement to the Processing of Personal Information about them;

2.3. "Data Subject" means any individual or legal entity;

2.4. "Operator" means any person who Processes Personal Information on behalf of a Responsible Party as a contractor or sub-contractor, in terms of a contract or mandate, not subject to the direct authority of the Responsible Party;

2.5. "Processing Notices" means a notice setting out the prescribed information that must be provided to Data Subjects before collecting his, her or its Personal Information, (also known as "Section 18 POPIA notices", "privacy notices" or "data protection notices" or consent forms).

2.6. “Personal Information” means Personal Information relating to any identifiable, living, natural person, and an identifiable, existing juristic person, including, but not limited to:

2.6.1. name, address, contact details, date of birth, place of birth, identity number, passport number;

2.6.2. bank details;

2.6.3. qualifications, expertise, employment details;

2.6.4. tax number;

2.6.5. vehicle registration;

2.6.6. dietary preferences;

2.6.7. financial details including credit history;

2.6.8. next of kin / dependants;

2.6.9. education or employment history; and

2.7. “Special Personal Information”, being including race, gender, pregnancy, national, ethnic or social origin, colour, physical or mental health, disability, criminal history, including offences committed or alleged to have been committed, membership of a trade union and biometric information, such as images, fingerprints and voiceprints, blood typing, DNA analysis, retinal scanning and voice recognition.

2.8. “Personnel” means Company Founder, partners, employees and any other person or third party

who may Process Personal Information on behalf of the Company.

2.9. “Processing, Process, Processed” means in relation to Personal Information, the collection, receipt, recording, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; merging, linking, as well as restriction, degradation, erasure or destruction of information; or sharing with, transfer and further Processing, including physical, manual and automatic and in relation thereto which may be held on a “Record” which means any recorded information housing Personal Information Processed by the Company, or its Personnel, regardless of form or medium.

2.10. “Purpose” means the underlying reason why a Responsible Party or Operator needs to Process a Data Subject’s Personal Information.

2.11“Responsible Party” means, in relation to POPIA, the person or legal entity who is Processing a Data Subject’s Personal Information.

2.12“Records” means all documents and records housing data, including held, created, used or processed by the Company, including Records containing personal Information.

3. SCOPE AND APPLICATION

This Policy applies to any persons who Process Personal Information on behalf of the Company, including Company founder, partners, employees and third parties, who will hereinafter be referred to collectively as "Personnel".

4. LAWFUL BASIS FOR PROCESSING

In terms of POPIA, where Personal Information is Processed such Processing must be done lawfully and in a reasonable manner that does not infringe on the privacy of the Data Subject. In order to discharge the above obligations, Personnel must comply with the Processing guides, rules and procedures set out below.

5. CONSENT

5.1. A Data Subject does not have to Consent to the Processing of their Personal Information where there is a lawful basis for such Processing. A lawful basis for Processing in terms of the Data Processing laws, is where:

5.1.1. the Processing is necessary to conclude a contract to which the Data Subject is a party and to perform contractual obligations or give effect to contractual rights;

5.1.2. the Processing is necessary in order to comply with a law or to comply with certain legal obligations imposed by a law;

5.1.3. the Processing is necessary to protect Company's legitimate interests or rights, the Data Subject's legitimate interests or rights or a third party's legitimate interests or rights, unless there is a good reason to protect the Data Subject's Personal Information that will override any such legitimate interests;

5.1.4. the Processing is necessary in order to perform a public duty or to perform tasks conducted in the public interest or the exercise of official authority.

5.2. Where there is no lawful basis for the Processing, then the Data Subject, has to Consent to the Processing.

5.3. Personnel must ensure that prior to Processing a Data Subject's Personal Information, that there is either a lawful reason for the Processing, or alternatively that the Data Subject has Consented to such Processing, which lawful reason will be described under the specific and informative Company Processing notices, or in the absence of a lawful reason, will call for the Data Subject's consent.

5.4. A Data Subject may withdraw their Consent as long as it provides the Company with a written notice of withdrawal of consent. This notice will be managed and actioned directly by the duly appointed Company Information Officer or Deputy Information Officer and which outcome will be relayed to the respective Personnel who has been Processing such Personal Information.

5.5. A Data Subject may not withdraw Consent where no Consent is required, such as, where the Company can show that there is a lawful basis for the Processing. In such a case the Data Subject may only object to such Processing, provided that a objection notice is given to the Company. This request will be managed and actioned directly by the Information Officer or Deputy Information Officer and which outcome will be relayed to the respective Personnel who has been Processing such Personal Information.

5.6 Where a Data Subject withdraws Consent or objects to Processing, the Company and the respective Personnel who have been Processing the impacted Personal Information, will have to stop Processing the Personal Information, unless the Company can show compelling legitimate grounds for the Processing which overrides the interests, rights and freedoms of the Data Subject, or the Processing is necessary for the establishment, exercise or defence of legal claims.

5.7. The Information Officer or Deputy Information Officer will at the time of the withdrawal or objection referred to above, explain to the Data Subject the effects and consequences of any withdrawal or objection and relay the outcome to the respective Personnel who has been Processing such Personal Information.

6. PURPOSE SPECIFIC

6.1. Personal Information:

6.1.1. may only be collected for a specified, explicit and legitimate purpose;

6.1.2. must only be used for the purpose for which it was collected and for no other purpose, unless the Data Subject has been informed of the other purposes;

6.1.3. may not be further Processed or used for any subsequent purpose unless that Personal Information is required for a similar purpose; and such Processing is compatible with the initial purpose.

6.2. The Company for the purposes of carrying out its business and related objectives, processes Personal Information belonging to a vast range of Data Subjects, including employees and staff, prospective employees and job applicants, students and interns, service providers and contractors, vendors, clients, customers, and other third parties, which processing is required for a variety of business-related purposes.

6.3. Examples of these purposes are described below:

6.3.1. to recruit and employ - employment;

6.3.2. to sell or purchase goods and services - procurement and supply chain;

6.3.3. concluding and managing a contract or business transaction - contract;

6.3.4. conducting criminal reference checks - legitimate interest;

6.3.5. risk assessments - legitimate interest;

6.3.6. insurance and underwriting purposes - legitimate interest;

6.3.7. assessing and Processing queries, enquiries, complaints, and/or claims - legitimate interest;

6.3.8. conducting credit checks - legitimate interest;

6.3.9. confirming, verifying and updating personal details - legitimate interest;

6.3.10. detection and prevention of fraud, crime, money laundering or other malpractices - legitimate interest;

6.3.11. conducting market or customer satisfaction research - legitimate interest;

6.3.12. direct marketing - marketing;

6.3.13. audit and record keeping purposes - legitimate interest;

6.3.14. managing debtor and creditors - legitimate interest;

6.3.15. complying with laws and regulations - statutory;

6.3.16. dealing with regulators - statutory;

6.3.17. paying taxes - statutory;

6.3.18. collecting debts or legal proceedings - statutory;

6.3.19. communications - legitimate interest;

6.3.20. managing employees - employment.

6.3.21. to facilitate AI-assisted tools for bookkeeping, reconciliation, and reporting services. Our objective is to deliver faster, more consistent, and more accurate work. No AI tool will autonomously post entries, make payments, submit tax returns, or take any external action affecting records. All AI-assisted output is reviewed and approved by a qualified person at PGCO Advisory before it is relied upon.

6.4. Company personnel must:

6.4.1. ensure that before Personal Information is processed, there is a valid and legitimate reason for such processing; and

6.4.2. advise all Data Subjects why the Personal Information is required, i.e., the purpose for the processing, which purpose will be described under the Company Processing notices, recorded on the Company website, which the Data Subject should be directed to.

7. ACCURACY

7.1. All Personal Information processed by the Company must be accurate and, where necessary, kept updated.

7.2. In order to ensure that Personal Information is accurate and is up to date, Personnel must:

7.2.1. take all and every reasonable step to ensure that all Personal Information that they process is accurate, having regard to the purposes for which it is processed, and where it is found to be inaccurate, that it is where possible, updated and rectified without delay;

7.2.2. implement procedures allowing Data Subjects to update their Personal Information;

7.2.3. send out regular communications to Data Subject requesting “updates to details”, which if responded to, should be acted on immediately by the relevant or responsible department;

7.2.4. where appropriate, and possible, ensure that any inaccurate or out-of-date records are updated, and the redundant information deleted or destroyed;

7.2.5. take note of the rights of the Data Subject in relation to updates and rectifications of Personal Information, recorded under the Company Processing Notices and give effect to any update request, when such request has been communicated through to it by the Information Officer.

8. DATA MINIMISATION

8.1. The Company may not process Personal Information which is not necessary for the Purpose for which the Personal Information is processed.

8.2. Personnel must:

8.2.1. ensure that when they process Personal Information on behalf of the Company, that it is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed; and

8.2.2. revisit all pre-populated questionnaires and forms which are currently used to collect or record Personal Information and consider the purpose or reason for the collection and thereafter analyse the types of Personal Information which is requested or collected and where of the view that certain Personal Information is not needed for the defined purpose, then such information should no longer be called for, collected and/or recorded and the relevant areas where this information is housed or asked for should be deleted.

9. TRANSPARENCY AND PROCESSING NOTICES

9.1. The Company has a duty to show that it has dealt with a Data Subject in a transparent manner.

9.2. In order to demonstrate transparency, the Company must refer all Data Subjects, to a specific and informed Processing Notice, in this case, consent forms, at the time when the Company collects and processes a Data Subject's Personal Information or within a reasonable period thereafter, which Consent forms must set out:

9.2.1. the types of Personal Information processed, and the purpose or reason for the processing;

9.2.2. the lawful basis relied upon for such processing or whether consent is required for the processing;

9.2.3. the period for which the Personal Information will be retained;

9.2.4. who the Personal Information will be shared with, including external or cross border transfers and the mechanism(s) relied upon for such transfer;

9.2.5. the security measures which are in place to protect the Personal Information, including where the Personal Information is sent to parties' cross border and the mechanism(s) relied upon for such protection; and

9.2.6. the respective rights of the Data Subject and how these rights may be exercised.

9.2.7. A Website Privacy and Cookies Notice which applies to any persons who make use of the Company websites, social media websites, emails, and other IT related communications facilities and platforms;

9.2.8. ensure that all Company documents, forms or other records (Records) that record or call for Personal Information contain the following Data Processing details:

Please note that in order for the Company to engage with you, it will have to Process certain Personal Information, which is your property, which Processing is described and explained under the specific and informative Company Consent forms, recorded for ease of reference on the Company's website, which we ask that you download and read. By providing us with the required Personal Information, such act will be taken as an indication that you have read and agree with the provisions described under the Consent forms and where applicable, you consent to the processing by us of your Personal Information.

10. GENERAL DUTIES: CONFIDENTIALITY, INTEGRITY AND SECURITY OF PERSONAL INFORMATION

10.1. In order to safeguard, secure and ensure the confidentiality and integrity of all Personal Information held by or under the control of the Company, the Company together with its Personnel must;

10.1.1. identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;

10.1.2. document the identified risks;

10.1.3. establish, in response to the identified risks, reasonable technical and organisational measures across all areas where Personal Information is held or stored, including electronic and physical mediums;

10.1.4. implement and maintain all approved and required measures across all areas where Personal Information is held or stored, including electronic and physical measures, all which are designed to minimise the risk of loss, damage, unauthorised destruction and/or unlawful access of Personal Information;

10.1.5. regularly verify that these measures are effectively implemented; and ensure that the measures are continually updated in response to new risks or deficiencies in previously implemented measures and safeguards, which measures include, where appropriate, among others, the following:

10.1.6. the pseudonymisation and encryption of Personal Information;

10.1.7. ongoing efforts to ensure the long-term confidentiality, integrity, availability and resilience of Personal Information recorded within the Company environment;

10.1.8. applications and processes which have the ability to rapidly restore the availability of and access to Personal Information in the event of a tangible or technical incident; and

10.1.9. procedures for the regular review, assessment and evaluation of the effectiveness of the technical and organisational measures taken to ensure the security of Processing, including regular IT Security Audits.

10.2. The duty to ensure data privacy, confidentiality and integrity of Personal Information starts when the Company initially interacts with a Data Subject and will continue throughout the relationship, until the purpose for the Processing of the Personal Information comes to an end.

11. RECORDS MANAGEMENT DUTIES: CONFIDENTIALITY, INTEGRITY AND SECURITY OF PERSONAL INFORMATION

11.1. In order to ensure the confidentiality and integrity of all Records, especially those that record or contain Personal Information which are held by the Company, and in order to safeguard and secure these Records, Personnel must ensure that:

11.2. All Processing of Personal Information activities and communications are reduced to writing and retained in a Record, which Record may either be electronic, or paper based;

11.2.1. Each Record created is classified, and then is housed in a folder (Folder), and where applicable in sub folders of the Folder being a storage area, either electronic or paper based and in turn each Folder / subfolder is given an appropriate title or Folder name using the Company naming convention and classification guide and template set out under “Annexure A”;

11.2.2. Folders and Records must be named in a consistent and logical manner so they can be located, identified and retrieved as quickly and easily as possible;

11.2.3. all Folders and Records must be stored and saved in a way that the contents are safeguarded and are identifiable as per the agreed Company naming convention and classification;

11.2.4. the name of the Folder and related sub folders and Records held in such Folders, together with the classification thereof must be recorded in a department specific records register which has to be compiled for each department, using the Company standard department management register (hereinafter referred to as the "Department Records Management Register"), as set out under "Annexure A", including the following details:

11.2.4.1. classification;

11.2.4.2. the name of the Folder and related Records;

11.2.4.3. format of the Folder and related Records;

11.2.4.4. location of Record - including physical or electronic location;

11.2.4.5. who has access to the Folder, and the Records;

11.2.4.6. status of the Folder and the Records;

11.2.4.7. retention period pertaining to the Folder and/or Records; and

11.2.4.8. destruction date of the Records, when appropriate;

11.2.5. their respective department head reviews their own department specific Department Records Management Register annually to ensure compliance with this Policy;

11.2.6. each department provides a copy of its Department Records Management Register to the Information Officer, annually, or on request.

11.3. Upon termination of employment, or change of job roles or responsibilities of Personnel, the affected line manager responsible for such Personnel must ensure that all access rights to any Company Folders or Records is removed immediately and that all Company assets used to access the Folders and or Records are returned to the Company, and that all physical access rights to the Company premises and facilities are revoked or cancelled.

12. RECORDS MANAGEMENT DUTIES: STORAGE OF RECORDS CONTAINING PERSONAL INFORMATION

12.1. In order to ensure the confidentiality and integrity of all paper-based Records that record or contain Personal Information, which are held by the Company, and in order to safeguard and secure these Records, Personnel must ensure that all paper-based Records:

12.1.1. which are housed in physical storage areas are labelled and the details recorded in the Department Management Register;

12.1.2. when in use, are not left around for others to access, and are not left in places where persons can view the contents e.g., on a printer or on unmanned desks;

12.1.3. are stored securely when not in use, in Folders, which in turn are placed in locked boxes, drawers, cabinets, or similar structures or containers;

12.1.4. that only Personnel who are required, on an operational and need to know basis, are given access to such Records and/or Folders; and

12.1.5. such Records and/or Folders are only removed from Company premises if such removal is recorded in the Department Records Management Register and when removed off site, such Records are safeguarded and kept confidential.

12.2. In order to ensure the confidentiality and integrity of all electronic Records that house or contain Personal Information, which are held by the Company, and in order to safeguard and secure these Records, Personnel must ensure that:

12.2.1. they comply with all applicable Company IT Policies and Procedures;

12.2.2. all electronic Records are stored and housed on Company servers that are protected by approved security software, and one or more firewalls under the direction of the Company IT Manager, and where transferred or uploaded to cloud computing services from computers, devices and applications, that these services have been approved by the Company IT Manager / Head of IT;

12.2.3. all devices where electronic Folders and/ or Records are stored, are password protected and that passwords are not written down or shared, irrespective of seniority or department, which passwords must be strong passwords that are changed regularly. If a password is forgotten, it must be reset using the applicable method;

12.2.4. all network devices and drives where electronic Folders and Records are stored have access control measures in place;

12.2.5. electronic Folders and Records are not stored on mobile devices and removable media, which includes, but is not limited to smart phones, tablets and iPad, Digital media, USB sticks, external hard drives, CDs, DVDs, DVDs, memory cards, tapes, unless the device is password protected and the content of such Record(s) is where possible encrypted;

12.2.6. where one needs to use and access the contents of an electronic Folder or Record, off site, which will not be accessed using Company secured servers, and which will be downloaded on to portable device for off-site working purposes, such person must only remove the Folders and/or Records or parts thereof if such removal is recorded in the Department Records Register; only the record(s) which are necessary for one's immediate needs are removed; where possible and feasible, the Personal Information to be removed is strongly encrypted; and

when removed off site, such Records are safeguarded and kept confidential and when no longer needed, that the removed Folder and/or Record, once dealt with is deleted from the portable device;

12.2.7. all electronic Records are regularly backed up using the Company provided systems and applications and in accordance with backup protocols. Such backups will be evaluated regularly in line with the Company standard backup procedures and protocols under the direction of the IT Manager / Head of IT;

12.2.8. all device screens, when not in use are always locked and password protected, especially when left unattended;

12.3. Electronic Records are only transmitted over secure networks, including wireless and wired networks.

12.3.1. In order to ensure the confidentiality and integrity of all Records that house or contain Personal Information, which are held by the Company, and in order to safeguard and secure these Records, Personnel must ensure that:

12.3.2. Records are shared with others on a "need to know" basis only. If Personnel are unclear on how to apply this requirement, the default position is that a conservative approach must be applied, i.e. information must be disclosed only to those people who have a legitimate business need for the information;

12.3.3. controls are in place to ensure that only personnel with proper authorisation and a need to know are granted access to Company systems and resources. Remote access shall be controlled through identification and authentication mechanisms;

12.3.4. proper controls are in place to authenticate the identity of Personnel or any third party who needs to access a Record, and all Personnel validate each person who requires access to the Record before allowing them access;

12.3.5. data used for authentication shall be protected from unauthorised access;

12.3.6. special needs for other access privileges will be dealt with on a request-by-request basis;

12.3.7. storage media containing Special Personal Information, or sensitive information (i.e. restricted or confidential information) shall be completely empty before reassigning that medium to a different user or disposing of it when no longer used. Simply deleting the data from the media is not sufficient. A method must be used that completely erases all data. When disposing of media containing data that cannot be completely erased it must be destroyed in a manner approved by the IT department.

12.3.8. Any attempts to bypass security controls or to obtain unauthorised access, or to make unauthorised use of another's account shall be considered a security breach or violation.

12.3.9. The use of any Company information or data for purposes other than for authorised business purposes shall be considered a security violation.

12.3.10. The use of any Company information or data for any unauthorised or illegal activity shall be considered a security breach or violation.

12.3.11. Any act, or failure to act, that constitutes or causes a security incident or creates a security exposure shall be considered a security breach or violation.

12.3.12. Any act, or failure to act that results in sensitive or business critical information being disclosed to an unauthorised person shall be considered a security breach or violation.

12.3.13. Any act, or failure to act that results in sensitive or business critical information being modified or destroyed, such that the Company is adversely impacted shall be considered a security breach or violation.

12.3.14. Any breach of this policy shall be considered a security breach or violation.

13. RECORDS MANAGEMENT DUTIES: RETENTION AND DISPOSAL OF RECORDS HOUSING PERSONAL INFORMATION

13.1. Folders and Records housing Personal Information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless the longer retention of the Folder or Record:

13.2. is required or authorised by law;

13.3. is required by the Company for lawful purposes related to its functions or activities;

13.4. is required by a contract between the parties thereto; is as per consent received from the Data Subject who owns the Personal Information; or

13.5. is required for the Operational Requirements of the Company.

13.6. Records housing Personal Information may be retained indefinitely for business, historical, statistical or research purposes provided that the Company has established appropriate safeguards against the Records being used for any other purposes.

13.7. Each Company department will be responsible for the correct management of their Folders and Records, including the closing and archiving of these Records when they are no longer required.

13.8. In order to ensure that the above duties are discharged, all Personnel must ensure that:

13.8.1. on an ongoing basis they manage the respective life cycles of Folders and Records under their control;

13.8.2. they establish what record retention periods and related requirements apply to the respective Folders and Records under their control, as per the Company Records Retention Policy;

13.8.3. the record retention periods, and related requirements are recorded in the department's relevant Department Records Management Register;

13.8.4. a Folder and Record is formally closed when the matter housed in the Folder or Record comes to an end, which is documented in the relevant Document Management Register;

13.8.5. a closed Folder or Record is moved to a dedicated archive storage area where the Folder or Record will be retained for the required retention period;

13.8.6. Folders and Records are only archived in secure storage media;

13.8.7. only authorised personnel are granted physical and system-based access to archived Folders and Records;

13.8.8. Folders and Records are archived in areas that are regularly backed up;

13.8.9. once the prescribed retention period in respect of an archived Folder or Record has expired, the Folder or Record is marked "for deletion or disposal";

13.9. before a Folder or Record is deleted or destroyed, the department head must obtain permission to delete or destroy said Folder or Record from the Information Officer, which will be reflected in the relevant department Records Management Register;

13.9.1. each department, once approval for the deletion / destruction of the Folder or Record has been received, will be responsible for the deletion or destruction of such archived

13.9.2. the legal / PAIA hold status must be indicated under the relevant Folder or Record in the relevant Document Management Register;

13.9.3. during a legal / PAIA hold procedure, the affected Folder or Record must not be destroyed, even if the retention period has expired;

13.9.4. the deletion / disposal of Folders and Records must ensure the permanent and complete deletion / disposal of all originals and reproductions (including both paper and electronically stored records);

13.9.5. the department head is responsible for documenting the destruction details under the relevant department Records Management Register.

14. OPERATORS

14.1. Where the Company makes use of an Operator, in terms of Sections 19-21 of POPIA, it must ensure that the Operator only uses the Personal Information per the mandate to Process issued by the Company, keeps the Personal Information placed under its control, confidential, secure and safe, and that a standard Company Operator Agreement / Addendum (hereinafter referred to as the "Operator Agreement / Addendum") is

concluded between the Company and the Operator. This Agreement sets out the above provisions and any other terms and rules which the Operator will have to follow when Processing Personal Information on behalf of the Company, and which Operator Agreement / Addendum is recorded on the Company website.

14.2. All Personnel must:

14.2.1. familiarise themselves with the standard Company Operator Agreement / Addendum; 14.2.2. ascertain who they use as Operators, now and in the future, include such details under an Operator register, and ensure that all such Operators sign the standard Company Operator Agreement / Addendum or a similar one which has been approved;

14.2.3. ensure that Operator Agreement / Addendum is followed by an Operator and that where an Operator Agreement / Addendum is breached, bring this to the attention of one's line manager and the Information Officer and following a decision reached by these parties, carry out the planned course of action, which ultimately must aim to protect and secure the Personal Information which is the subject matter of that Operator Agreement / Addendum.

14.3. The Company utilises specific Operators (sub-processors) to deliver services. These include:

- Xero South Africa (Pty) Ltd for cloud accounting (processed in South Africa / Australia);
- Dext Software for receipt / bill capture (processed in the United Kingdom);
- SimplePay for payroll (processed in South Africa);
- Anthropic, PBC for AI-assisted bookkeeping (processed in the United States).

14.4. When utilising these Operators, the Company applies strict safeguards, including human review and approval of all AI-assisted work, internal audit trails, restriction of access to authorised PGCO personnel only, and ensuring Operators hold industry-standard security accreditation (such as SOC 2 Type II).

15. SHARING PERSONAL INFORMATION WITH THIRD PARTIES

15.1. The Company may not share Personal Information with third parties, unless:

15.1.1. there is a legitimate business need to share the Personal Information; or

15.1.2. the Data Subject has been made aware that their Personal Information will be shared with others and has, where required, given consent to such sharing; or

15.1.3. the person receiving the Personal Information has agreed to keep the Personal Information confidential and to use it only for the purpose for which it was shared under the standard Company Personal Information transfer agreement or where acting as an Operator.

15.2. In order to ensure that the above takes place, Personnel must ensure:

15.2.1. that where Personal Information is shared externally with a third party, there is a legitimate business need to share the Personal Information; or the Data Subject has been made aware that their Personal Information will be shared with others and has, where required, given consent to such sharing;

15.2.2. in the absence of the above two situations, has signed the standard Company Personal Information transfer agreement, which is concluded with the recipient, before receipt of the Personal Information;

15.2.3. that where Personal Information is shared with an Operator, that the standard Company Operator Agreement / Addendum is concluded with the Operator before receipt of the Personal Information;

15.2.4. that any requested deviations for the standard Company Personal Information transfer agreement or the Operator Agreement / Addendum are vetted and approved by the Group HR or Group Internal Auditing departments beforehand;

15.2.5. when sending emails that contain Personal Information, that they are marked “confidential”, do not contain the Personal Information in the body of the email, whether sent or received, but rather placed in an attachment, which attachment is password protected or encrypted before being transferred electronically;

15.2.6. that Personal Information is not transferred or sent to any entity not authorised directly to receive it;

15.2.7. that where Personal Information is to be sent by facsimile transmission, that the recipient has been informed in advance of the transmission and that he or she is waiting by the fax machine to receive the data;

15.2.8. that where Personal Information is transferred physically, whether in hardcopy form or on removable electronic media, that it is passed directly to the recipient or sent using recorded deliver services and housed in a suitable container marked “confidential”;

15.2.9. that where Personal Information is shared internally, that adequate measures are put in place to protect the confidentiality and integrity of such information.

16. CROSS BORDER TRANSFERS OF PERSONAL INFORMATION

16.1. The Company may not transfer Personal Information to another party who is situated outside South Africa, unless:

16.1.1. the Data Subject Consents (under POPIA);

16.1.2. the transfer is necessary in order to perform a contract between Company and a Data Subject, or for reasons of public interest, or to establish, exercise or defend legal claims or to protect the vital or legitimate interests of the Data Subject in circumstances where the Data Subject is incapable of giving Consent;

16.1.3. the country where the Personal Information is being transferred to, provides the Data Subject with the same level of protection as is housed under the data processing laws applicable in South Africa; or alternatively

16.1.4. the Company has concluded a Personal Information data transfer agreement with the recipient of the Personal Information, either in the form of a standard binding corporate rule, or an Operator Agreement / Addendum or a Personal Information transfer agreement, which sets out the rules that apply to the receipt and the subsequent Processing of that Personal Information.

16.2. In order to ensure that the above is followed, Personnel may not transfer Personal Information to areas outside South Africa, unless one of the following controls and safeguards are in place:

16.2.1. the South African Data Privacy /Personal Information Regulator has issued an "adequacy decision" confirming that the territory or country where the Company proposes transferring the Personal Information to, has adequate Data Protection laws in place which will afford the Data Subject with the same level of protection as that under POPIA;

16.2.2. the standard Company Personal Information data transfer agreement or Operator Agreement / Addendum has been concluded with the recipient of the Personal Information;

16.2.3. the Data Subject has given Consent (POPIA) to the proposed transfer, having been fully informed of any potential risks; or

16.3. the transfer is necessary in order to perform a contract between the Company and a Data Subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject in circumstances where the Data Subject is incapable of giving Consent (POPIA).

16.4. Cross-border transfers include the transfer of information to Anthropic, PBC on servers in the United States. The Company ensures that it has satisfied itself that Anthropic is subject to contractual terms providing protection substantially similar to POPIA, including strict data-security obligations and a contractual prohibition on using Company data to train AI models.

17. DIRECT MARKETING

17.1. Direct marketing, including unsolicited direct electronic marketing is prohibited unless the Data Subject has consented to the receipt of this marketing material.

17.2. In order to ensure that direct marketing is sent out in a lawful manner, all Personnel must ensure that:

17.2.1. all Company customers, when approached or dealt with for the first time, are given the opportunity in an informal manner to agree or disagree to the receipt of any Company direct marketing material and that where consent is granted, that the details of the customer are set out under a "consented to" direct marketing data

base, and when marketing material is sent to these Data Subjects, that the material houses an “opt out” form, allowing the Data Subject to opt out of any further marketing material should it so elect;

17.2.2. before direct marketing is sent to a non-customer that such person provides their consent thereto, which will be in the form of the prescribed “opt in” notice on the consent form;

17.2.3. when marketing material is sent to Data Subjects, who have “opted in” that the material contains an “opt out” option as well, allowing the Data Subject to opt out of any further marketing material; and

17.2.4. when a Data Subject exercises their right to object to receiving direct marketing, in the form of an opt out, that such opt out is recorded and given effect to, and that no further direct marketing is sent to the opted-out customer.

17.2.5. All Personnel, especially those who engage in direct marketing must familiarise themselves with the Company marketing opt in and opt out requirements.

18. REPORTING PERSONAL INFORMATION BREACHES

18.1. In the event of a Personal Information breach, the Company has a duty to give notice of such breach to the Regulator who is in charge of POPIA, being the Information Regulator, and to the Data Subject(s) whose Personal Information has been affected as a result of such breach.

18.2. The Company has put in place appropriate procedures to deal with any Personal Information breach and will notify the Information Regulator and/or the Data Subjects, as the case may be, when it is legally required to do so of any breach.

18.3. Personnel have a duty to:

18.3.1. immediately report through to the Information Officer, any suspected or known Personal Information breach; using the prescribed Company data breach report, which report format is annexed hereto marked “Annexure B” . The report must contain the following details:

18.3.1.1. categories and approximate number of Data Subjects concerned;

18.3.1.2. categories and approximate number of Personal Information records concerned;

18.3.1.3. the likely cause of and the consequences of the breach; and

18.3.1.4. details of the measures taken, or proposed to be taken, to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

18.3.2. keep such information strictly private and confidential;

18.3.3. ensure that they do not deal with any persons in relation to the Personal Information breach, including any officials or investigators, noting that only the Information Officer with the approval of the CEO or the Company's Board has the right to report any Personal Information or security breach to the Information Regulator and/or the affected Data Subjects, as the case may be and to deal with any person in connection with such matter.

19. DATA SUBJECT RIGHTS AND REQUESTS

19.1. A Data Subject has rights under POPIA in relation to their Personal Information, including the right to:

19.1.1. withdraw Consent;

19.1.2. object to Processing;

19.1.3. obtain confirmation of Processing and/or access to Personal Information;

19.1.4. amend, update and delete Personal Information;

19.1.5. object to direct marketing;

19.1.6. be notified of a personal information breach; and

19.1.7. complain about the processing of Personal Information.

19.2. Personnel must:

19.2.1. familiarise themselves with the Data Subjects' rights, and the related processes and forms which need to be followed and completed in order to access these rights;

19.2.2. take note of and give effect to these processes;

19.2.3. in particular note that where a Data Subject seeks advice on what Personal Information the Company holds and which pertains to that Data Subject or where the Data Subject is desirous of accessing this Personal Information, that such right has to be exercised using the "request for access to information" procedure which is described the Promotion of Access to Information Act, 2 of 2000, ("PAIA"), and which request procedure is more fully set out under the Company's PAIA Manual available on the Company website.

19.2.4. where asked by any Data Subject to give effect to these rights, not deal with the request directly but instead direct the Data Subject to the relevant process and form on the Company website and aid in so far as completing the form only.

20. THE RIGHT TO COMPLAIN

20.1. A Data Subject has the right to lodge a complaint with regards to the Processing of their Personal Information.

20.2. The Company has established for this purpose, an internal compliant resolution procedure.

20.3. Should a Data Subject wish to submit a complaint, Personnel must, if contacted by the Data Subject, ask the Data Subject to provide a written letter about the compliant, and to submit the complaint letter to the Information Officer.

20.4. On receipt of the complaint, the Information Officer will attempt to hear and resolve the matter internally and failing resolution will provide the Data Subject with a non-resolution notice.

20.5. If the Information Officer and Data Subject are able to resolve the matter, a record setting out the solution will be compiled, and signed by the parties and any other affected persons provided with details of the resolution.

20.6. Where the parties are unable to resolve the matter, the Data Subject on receipt of the non- resolution notice, will have the right to refer the complaint to the Information Regulator.

21. GOVERNANCE

21.1.1. The Company has appointed Information Officer(s) and Deputy Information Officer(s), as outlined who will be responsible for the following:

21.1.2. developing, constructing and once prepared, implementing and overseeing an enterprise-wide Personal Information Processing framework and related roadmap including various Personal Information Processing procedures and policies, including this Policy;

21.1.3. monitoring compliance with this Policy, the various Personal Information Processing procedures and the Data Processing law;

21.1.4. providing all Personnel with the necessary and required Personal Information Processing training;

21.1.5. providing ongoing guidance and advice on Personal Information Processing;

21.1.6. conducting Personal Information impact assessments when required, including base line risk assessments of all the Company's Personal Information Processing activities;

21.1.7. ensuring that all operational and technological Personal Information and data protection standards are in place and are complied with;

21.1.8. working closely with IT in order to ensure that appropriate technological and operational measures have been implemented in order to ensure the safety and security of all electronically stored Personal Information;

21.1.9. receiving and considering reports from IT about compliance with all technological and operational data protection standards and protocols;

21.1.10. be entitled and have authorisation in conjunction with the Company HR function, to initiate disciplinary proceedings against Personnel who breach any technological and/or organisational and/or operational data protection standard, rule, custom, instruction, policy, practice and/or protocol (verbal, in writing or otherwise), including this Policy;

21.1.11. .attend to requests and queries from Data Subjects, including requests for access to their Personal Information;

21.1.12. consulting with and/or co-operating with any regulators, investigators, or officials who may be investigating a Personal Information or data privacy matter.

21.1.13. All queries and concerns in relation to the Processing of Personal Information within the Company operations or concerning Company activities, must be taken up with the Information or Deputy Information Officers.

21.2. The Company's IT department will be responsible for the following:

21.2.1. conducting cyber security risk assessments including base line risk assessments of all the Company information technology activities;

21.1.2. ensuring that adequate and effective IT operational and technological data protection procedures and standards are in place in order to address all IT security risks;

21.1.3. ensuring that all systems, services and equipment used for Processing and/or storing data adheres to internationally acceptable standards of security and data safeguarding, and is regularly updated to continue to comply with such standards;

21.1.4. issuing appropriate, clear, and regular rules and directives, whether for the Company as a whole or a particular part of it, department, person or level of person in relation to any aspect of the Company work, including password protocols, data access protocols, levels of persons who enjoy access to certain data sign-on procedures, password safeguarding protocols, sign-on and sign-off procedures, log-on and log-off procedures; the description of accessories, applications and equipment that will or may be used, and/or that may not be used under any circumstances, and the like.

21.1.5. evaluate any third-party services which the Company is considering or may acquire to Process or store data, e.g., cloud computing services and ensuring that appropriate and effective operational and technological data protection procedures and standards are in place in order to address all IT security risks which may present themselves in respect of these external service providers.

22. TRAINING

22.1. The Company will conduct regular training sessions covering the contents of the data privacy laws and the Company related Personal Information Processing policies and procedures, which will be available to all Personnel.

22.2. Personnel must:

22.1.1. attend the scheduled and offered training;

22.1.2. do all that is necessary in order to understand the data privacy laws and how they may impact on the Company Personal Information Processing activities;

22.1.3. familiarise themselves with the Company Personal Information Processing policies, procedures and prescribed forms;

22.1.4. ensure that they Process Personal Information in accordance with the Data Processing laws, this Policy, the training, the related policies and procedures and/or any guidelines issued by the Company from time to time.

23. NON-COMPLIANCE

23.1. Compliance with this Policy and any related procedures and policies is mandatory.

23.2. Any transgression of this Policy, and any related procedures and policies, will be investigated and may lead to action being taken against the transgressor.

23.3. Further information on the relevant data protection laws, POPIA, the Company Processing of Personal Information procedures and issues, and Processing Notices, including specific practical guidance on issues of particular relevance to Personnel, can be found on the Company's website.

24. VERSION AND AMENDMENTS

This Policy is effective as of 1st July 2026.

The Company reserves the right to amend the Policy at any time, for any reason, and without notice to you other than the posting of the updated Policy on the Company Website.

We therefore request that you visit our website frequently in order to keep abreast with any changes.

Signed at Sandton on this 9th day of June 2026.

_____

Information Officer

ANNEXURE A

DOCUMENTS AND RECORDS CLASSIFICATION INSTRUCTIONS AND REGISTER FORMATS CLASSIFICATION INSTRUCTIONS

Any person who collects, uses, stores, or transmits Documents and Records has a responsibility to maintain and safeguard such Data.

The first step in establishing the safeguards that are required for a particular type of Documents and Records is to determine the level of sensitivity applicable to such Data. Documents and Records classification is a method of assigning such categories and thereby determining the extent to which the Documents and Records needs to be governed, controlled and secured.

The responsibility for the classification of Documents and Records rests with the Documents and Records owner/ business unit where the documents have their origin.

Documents and Records classification, in the context of information security, also addresses the impact to the Group should such classified Documents and Records be disclosed, altered, or destroyed without authorization.

The classification of Documents and Records helps determine what baseline security controls are appropriate for safeguarding that Data. All Group Documents and Records are categorized into one of four sensitivity classifications:

Proprietary Data

Documents and Records should be classified as Proprietary when this information is restricted to management approved internal access and protected from external access. Unauthorized access could influence the Company's operational effectiveness, cause a financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is therefore vital.

Examples of this type of Documents and Records includes passwords and information on corporate security procedures; know-how used to process client information; Standard Operating

Procedures used in all areas of Company business; all Company-developed intellectual property, whether used internally or in transactions with third parties.

Confidential Documents and Records

Documents and Records should be classified as Confidential when the unauthorized disclosure, alteration or destruction of that Documents and Records could cause a significant level of risk to the Company or its affiliates. Examples of Confidential Documents and Records include Documents and Records protected by privacy regulations and Documents and Records protected by confidentiality agreements. This also includes information received from third parties in any form for processing and use by any Group Company. The highest level of security controls should be applied.

Access to Confidential Documents and Records must be controlled from creation to destruction and will be granted only to those persons affiliated to the respective Group Company who require such access to perform their job ("need to know"). Access to Confidential Documents and Records must be individually requested and then authorized by the Documents and Records Owner who is responsible for the data.

Confidential Documents and Records is highly sensitive and may have personal privacy considerations or may be restricted by a statute. In addition, the negative impact on the institution should this Documents and Records be incorrect, improperly disclosed, or not available when needed is typically very high.

Examples of Confidential / Restricted Documents and Records include salaries and other personnel data; accounting Documents and Records and internal financial reports; Company business plans; confidential customer business Documents and Records; confidential contracts; and any information shared thereof.

Such Confidential Documents and Records shall also be protected in terms of the Protection of Personal Information Act, 4 of 2013, and in accordance with the Company POPIA Policy.

Internal / Private Documents and Records

This type of Documents and Records can be defined as any information that is proprietary or produced only for use by members of the Group who have a legitimate purpose to access such data.

Documents and Records should be classified as Internal / Private when the unauthorized disclosure, alteration or destruction of that Documents and Records could result in a moderate level of risk to the Company or its affiliates. By default, all information assets that are not explicitly classified as Confidential or Public Documents and Records should be treated as Internal / Private Data. A reasonable level of security controls should be applied to Internal Data.

Access to Internal / Private Documents and Records must be requested from, and authorized by, the Documents and Records Owner who is responsible for the data. Access to Internal / Private Documents and Records may be

authorized to groups of persons by their job classification or responsibilities ("role- based" access) and may also be limited by one's department.

Internal / Private Documents and Records is moderately sensitive in nature. Often, Internal / Private Documents and Records is used for making decisions, and therefore it is important this information remain timely and accurate. The risk for negative impact on the Group should this information not be available when needed is typically moderate. Examples of Internal / Private.

Documents and Records include official Company records such as financial reports, human resources information, some research data, unofficial employee records, budget information, internal operating procedures and operational manuals, internal memoranda, emails, reports and other documents, and technical documents such as system configurations and floor plans.

Public Documents and Records

This type of Documents and Records can be defined as any information that may or must be made available to the public, with no legal restrictions on its access or use.

Documents and Records should be classified as Public when the unauthorized disclosure, alteration or destruction of that Documents and Records would result in little or no risk to the Company and its affiliates. While little or no controls are required to protect the confidentiality of Public Data, some level of control is required to prevent unauthorized modification or destruction of Public Data.

Public Documents and Records is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions. The integrity of Public Documents and Records should be protected. The appropriate Documents and Records Owner must authorize replication or copying of the Documents and Records to ensure it remains accurate over time. The impact on the company, should Public Documents and Records not be available is typically low (inconvenient but not debilitating). Examples of Public Documents and Records include directory information, course information and research publications.

DATA COLLECTIONS

Data Owners may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of an employee's address and ID number, the data collection should be classified as Confidential even though the employee's name and address may be considered Public Data.

DETERMINING CLASSIFICATION

The aim of information security is to protect the confidentiality, integrity and availability of information assets and systems. Data classification reflects the level of impact to the Group if confidentiality, integrity or availability of the data is compromised.

POTENTIAL IMPACT	LOW	MODERATE	HIGH
Security Objective			
Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.
Integrity - Guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.
Availability - Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.

INFORMATION HANDLING REQUIREMENTS

The table below defines the required security controls for handling, transmitting, dispatching, protecting, and reproducing classified information assets:

SECURITY CONTROL	INFORMATION CLASSIFICATION			
Area	**Proprietary Data**	**Confidential**	**Internal / Private Data**	**Public data**
Access Control	Viewing and modification restricted to authorized individuals as needed for business-related roles. Data Owners or custodian grants permission for access, plus approval from line manager. Authentication and authorization required for access. Confidentiality agreement required.	Viewing and modification restricted to authorized individuals as needed for business-related roles. Data Owners or custodian grants permission for access, plus approval from line manager. Authentication and authorization required for access. Confidentiality agreement required.	Viewing and modification restricted to authorized individuals as needed for businessrelated roles. Data Owner or custodian grants permission for access, plus approval from the line manager. Authentication and authorization required for access.	No restrictions for viewing.
Copying and Printing (applies to both paper and electronic)	Data shall only be printed when there is a legitimate need. Copies shall be limited to individuals authorized to access the data and have signed a confidentiality	Data shall only be printed when there is a legitimate need. Copies shall be limited to individuals authorized to access the data and have signed a	Data shall only be printed when there is a legitimate need. Copies shall be limited to individuals on a need-to know basis. Information shall not be left	No restrictions

	agreement. Information shall not be left unattended on a printer / desk. Control access to print output on copier. Copies shall be labelled as per categorization "Confidential" or "Proprietary".	confidentiality agreement. Information shall not be left unattended on a printer / desk. Control access to print output on copier. Copies shall be labelled as per categorization "Confidential" or "Proprietary".	unattended on a printer / desk. Control access to print output on copier.	
Physical Security	**Hardcopy**: Secure in locked cabinet or location with appropriate physical controls. Physical access shall be monitored, logged, and authorized individuals.	**Hardcopy**: Secure in locked cabinet or location with appropriate physical controls. Physical access shall be monitored, logged, and authorized individuals.	**Hardcopy**: Secure in locked cabinet or location with appropriate physical controls.	System shall be locked or logged out when unattended.
Information storage	Storage on a secure server, cloud **recommended**. Storage in a secure data Centre or cloud **recommended**. Should not store on an individual's workstation, mobile device (cell phones,	Storage on a secure server or cloud **recommended**. Storage in a secure data Centre or cloud **recommended**. Should not store on an individual's workstation, mobile device (cell phones,	Storage on a secure server or cloud **recommended**. Storage in a secure data Centre or cloud **recommended.** Lock screen when unattended.	Storage in a secure server recommended. Storage in a secure Data Centre. Lock screen when unattended.

	laptops, iPad, etc.) or removal devices (USB, external hard drives). If stored on a workstation or mobile device, shall use full disk encryption. Encryption on backup media required. Use restricted access folders. **Mandatory:** file password protection for sensitive files at document level. Hardcopy: Secure in locked cabinet or location with appropriate physical controls.	laptops, iPad, etc.) or removal devices (USB, external hard drives). Hardcopy: Secure in locked cabinet or location with appropriate physical controls. Use restricted access folders. **Mandatory:** file password protection for sensitive files at document level.		
Transmission	Encryption required. Cannot transmit via email unless encrypted and secure with a digital signature.	Encryption required.	Encryption required.	No restrictions.
Remote access to systems hosting data	Access is restricted to local network or VPN. Confidentiality	Access is restricted to local network or VPN.	Access is restricted to local network or VPN.	No restrictions.

	agreement required for remote access by third party for technical reasons.			

DOCUMENT RECORDS MANAGEMENT REGISTER FORMAT

Author:		
Title:		
Duration:		
Classification:		
Reason for reviewing documents and Personal Information:		
2. File Names housed in folder		
Primary Folder name	**Location**	
Sub Folder name	**Contents**	
Sub Folder name	**Contents**	
Sub Folder name	**Contents**	
Date Created:	**Signed:**	**Version:**
	Date amended:	

ANNEXURE B

INCIDENT INVESTIGATION FORM

This incident report is to be used for all incidents relating to privacy and information security incident management.

Definition of an incident: A threat or event that compromises, damages, or causes a loss of confidential or protected information.

Confidential information: includes proprietary, technical, business, financial, joint-venture, customer and employee information that is not available publicly. It is the employee's responsibility to know what information is confidential and to obtain clarification when in doubt.

Person reporting the incident (can remain anonymous)	
Manager	
Date and time incident occurred	
Date and time incident reported	
Division	
Site	

INCIDENT SUMMARY (SHORT STATEMENT OF EVENT)

INCIDENT INVESTIGATION

The following sections are intended to assist you to clarify the sequence of events immediately preceding the incident. They expand on the details already provided in the summary. Additional pages/ documents can be attached where required.

WHO WAS INVOLVED?

ARE THERE WITNESSES?

WHAT HAPPENED?

PGCO
Accounting I Tax I Advisory
www.pgco.co.za

WHEN DID THE INCIDENT OCCUR?

WHERE DID THE INCIDENT OCCUR?

THE EXISTENCE OR LOCATION OF ANY PROOF THAT MAY EXIST?

THE EXTENT OR CONSEQUENCES OF THE DAMAGE / COMPROMISE

SIGNATURE: _____

DATE: _____

PGCO
Accounting | Tax | Advisory
www.pgco.co.za

PGCO Advisory Incorporated

Johannesburg: 1st Floor | 155 West Street | Sandton | 2196 | South Africa
Durban: 7 Menston Road | Westville | Durban | 3629 | South Africa

+27 11 568 0755 info@pgco.co.za pgco.co.za

PROMOTION OF ACCESS INFORMATION ACT 2 OF 2000 (AS AMENDED)

PAIA MANUAL

PGCO
Accounting | Tax | Advisory
www.pgco.co.za

Contents

1. LIST OF ACRONYMS AND ABBREVIATIONS

1.1 **"CEO"**	Chief Executive Officer
1.2 **"DIO"**	Deputy Information Officer
1.3 **"IO"**	Information Officer
1.4**"Minister"**	Minister of Justice and Correctional Services
1.5"**PAIA"**	Promotion of Access to Information Act No. 2 of 2000 (as Amended)
1.6**"POPIA"**	Protection of Personal Information Act No.4 of 2013
1.7**"Regulator"**	Information Regulator
1.8 **"Republic"**	Republic of South Africa

2. PURPOSE OF THE PAIA MANUAL

Section 32 of the Constitution of the Republic of South Africa, No. 108 of 1996 ("the Constitution") provides:

(1) Everyone has the right of access to –

(a) any information held by the state; and

(b) any information that is held by another person and that is required for the exercise or protection of any rights.

(2) National legislation must be enacted to give effect to this right and may provide for reasonable measures to alleviate the administrative and financial burden on the state.

The Promotion of Access to Information Act, No.2 of 2000 ("the Act"), gives effect to section 32 of the Constitution, that enshrines the constitutional right of access to any information held by the State and any information that is held by another person and that is required for the exercise or protection of any rights.

Where a request is made in terms of this Act, a private or public body, as contemplated in the Act, to whom the request is made is obliged to provide access to the information, except where the Act expressly provides that the information must not be released. The Act sets out the requisite procedural issues attached to such request. This manual therefore applies to requests for access to records held by PGCO Advisory Incorporated, as the personal liability company contemplated under the Act.

This PAIA Manual is useful for the public to-

2.1 check the categories of records held by a body which are available without a person having to submit a formal PAIA request;

2.2 have a sufficient understanding of how to make a request for access to a record of the body, by providing a description of the subjects on which the body holds records and the categories of records held on each subject; know the description of the records of the body which are available in accordance with any other legislation;

2.3 access all the relevant contact details of the Information Officer and Deputy Information Officer who will assist the public with the records they intend to access;

2.4 know the description of the guide on how to use PAIA, as updated by the Regulator and how to obtain access to it;

2.5 know if the body will process personal information, the purpose of processing of personal information and the description of the categories of data subjects and of the information or categories of information relating thereto;

2.6 know the description of the categories of data subjects and of the information or categories of information relating thereto;

2.7 know the recipients or categories of recipients to whom the personal information may be supplied;

2.8 know if the body has planned to transfer or process personal information outside the Republic of South Africa and the recipients or categories of recipients to whom the personal information may be supplied; and

2.9 know whether the body has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

3. WHO MAY REQUEST INFORMATION IN TERMS OF THE ACT

Any person who requires information for the exercise or protection of any rights, may request information from PGCO Advisory Incorporated. Section 50 of the Act states that:

(1) A requester must be given access to any record of a private body if –

a. that record is required for the exercise or protection of any rights;

b. that person complies with the procedural requirements in this Act relating to a request for access to that record; and

c. access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

3.1 Key contact details for access to information of PGCO Advisory Incorporated:

Any person who wishes to request any information from PGCO Advisory Incorporated with the aim of protecting or exercising a right may contact the information officer whose contact details are as follows:

3.1.1. Requests to be addressed to: PGCO Advisory Incorporated Information Officer

3.1.2. Postal addresses: 1st Floor, 155 West St, Sandton, 2196

Phone number: +27 11 568 0755

+ 27 31 100 0755

E-mail address: yulesen@pgco.co.za

Website: www.pgco.co.za

3.2 Prescribed access form

In terms of section 53, a request for access to a record held by PGCO Advisory Incorporated must be made in the prescribed form to PGCO Advisory Incorporated at the address, or electronic mail address given above. The form requires you, as the requester to provide the following information:

3.2.1. sufficient information to enable the identification of the requester;

3.2.2. sufficient information to enable the identification of the record(s) requested;

3.2.3. the form of access required;

3.2.4. the requester's postal address or fax number;

3.2.5. identification of the right sought to be exercised or protected;

3.2.6. an explanation as to why the record is required to exercise or protect that right;

3.2.7. the way the requester wishes to be informed of the decision on the request, if in a manner in addition to written notification; and

3.2.8. if the request is made on behalf of a person, the submission of proof of the capacity in which the requester makes the request, to the satisfaction of PGCO Advisory Incorporated Information Officer, Yulesen Gounden, Managing Director of PGCO Advisory Incorporated.

Refer to FORM 2 to this manual for the format of the prescribed form. Requesters should please note that all the information as listed above should be provided, failing which the process will be delayed while PGCO Advisory Incorporated requests such additional information. The prescribed time periods will not commence until all pertinent information has been furnished to PGCO Advisory Incorporated by the requester.

3.3 Prescribed fees

Payment of fees is regulated in terms of section 54 of the Act. The Regulations to the Act provide for two types of fees:

3.3.1. Request fee: This is a non-refundable administration fee paid by all requesters. It is paid before the request is considered.

3.3.2. Access fee: This is paid by all requesters only when access is granted. This fee is intended to reimburse the private body for the costs involved in searching for a record and preparing it for delivery to the requester.

3.3.3. PGCO Advisory Incorporated may withhold a record until the request fee and the deposit (if applicable) have been paid. Refer to FORM 3 below for a list of applicable fees.

3.3.4. Requester

Written notice must be given to a requester of the request fee and amount to be paid before the request may be further processed.

If the search for a record, or preparation of the record for disclosure will require more than the prescribed hours, the requester may be required to pay a deposit, not being more than one third of the access fee that would be payable if the request is granted. If the request is declined, the deposit must be repaid to the requester.

The notice given to the requester must advise the requester that s/he has a right to apply to court against the payment of the request fee or deposit and should also advise of the procedure of the matter.

4. GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE

4.1 The Regulator has, in terms of section 10(1) of PAIA, as amended, updated and made

available the revised Guide on how to use PAIA ("Guide"), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.

4.2 The Guide is available in each of the official languages and in braille.

4.3 The aforesaid Guide contains the description of-

4.3.1 the objects of PAIA and POPIA;

4.3.2 the postal and street address, phone and fax number and, if available, electronic mail address of-

4.3.2.1 the Information Officer of every public body, and

4.3.2.2 every Deputy Information Officer of every public and private body designated in terms of section 17(1) of PAIA1 and section 56 of POPIA;

4.3.3 the manner and form of a request for-

4.3.3.1 access to a record of a public body contemplated in section 113; and

4.3.3.2 access to a record of a private body contemplated in section 504;

4.3.3.3 the assistance available from the IO of a public body in terms of PAIA and POPIA; 4.3.3.4 the assistance available from the Regulator in terms of PAIA and POPIA;

4.3.4. all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging-

4.3.4.1 a complaint to the Regulator; and

4.3.4.2 an application with a court against a decision by the information officer of a public body, a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body;

4.3.5 the provisions of sections 14 and 51 requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;

4.3.6. the provisions of sections 15 and 52 providing for the voluntary disclosure of categories of records by a public body and private body, respectively;

4.3.7 the notices issued in terms of sections 22 and 54 regarding fees to be paid in relation to requests for access; and

4.3.8 the regulations made in terms of section 92.

4.4 Members of the public can inspect or make copies of the Guide from the offices of the public and private bodies, including the office of the Regulator, during normal working hours.

4.5 The Guide can also be obtained-

all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging-

4.5.1. a complaint to the Regulator; and

4.5.2. an application with a court against a decision by the information officer of a public body, a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body;

4.5.3 the provisions of sections 14 and 51 requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;

4.5.4. the provisions of sections 15 and 52 providing for the voluntary disclosure of categories of records by a public body and private body, respectively;

4.5.5. the notices issued in terms of sections 22 and 54 regarding fees to be paid in relation to requests for access; and

4.5.6. the regulations made in terms of section 92.

5. CATEGORIES OF RECORDS

5.1 EMPLOYEE RECORDS

5.1.1. Records found in this division contain information of employees that include the following: 5.1.1.1. any personal records provided to PGCO Advisory Incorporated by the employee/personnel;

5.1.1.2. any records a third party has provided to PGCO Advisory Incorporated about its personnel;

5.1.1.3. conditions of employment and other personnel-related contractual and quasi-legal records;

5.1.1.4. internal evaluation records.

5.2 CLIENT RELATED RECORDS

Clients include both juristic and natural entities that receive a service from PGCO Advisory Incorporated. This information includes:

5.2.1. any records a client has provided to a third party acting for and on behalf of PGCO Advisory Incorporated;

5.2.2. any records a third party has provided to PGCO Advisory Incorporated and

5.2.3. records generated by or within PGCO Advisory Incorporated pertaining to the client, including transactional records.

5.3 PGCO ADVISORY INCORPORATED RECORDS

This category of records relates, but is not limited to, the following information:

5.3.1. Financial records

5.3.2. Operational records

5.3.3. Databases

5.3.4. Information technology

5.3.5. Marketing records

5.3.6. Internal correspondence

5.3.7. Product records

5.4. Each request will be evaluated on its own merits. If any record falls within any of the

categories of exemptions, then such a request will be refused.

5.5 OTHER PARTIES

PGCO Advisory Incorporated may possess records pertaining to other parties, including without limitation, contractors, suppliers, subsidiary/holding/sister companies, joint venture companies, service providers. Alternatively, such other parties may possess records that can be said to belong to PGCO Advisory Incorporated. The following records fall under this category:

5.5.1. Personnel, client or PGCO Advisory Incorporated records which are held by another party as opposed to being held by PGCO Advisory Incorporated; and

5.5.2. Records held by PGCO Advisory Incorporated pertaining to other parties, including without limitation financial records, correspondence, contractual records, records provided by the other party, and records third parties have provided about the contractors/suppliers.

5.6 RECORDS AVAILABLE IN TERMS OF OTHER LEGISLATION

The requester may also request information that is available in terms of legislation, such as the following:

CATEGORY OF RECORDS	APPLICABLE LEGISLATION
Personnel information as far as it is allowed in terms of these Acts	• Basic Conditions of Employment Act 75 of 1997 • Compensation for Occupational Injuries & Diseases Act 130 of 1993) • Employment Equity Act 55 of 1998 • Labour Relations Act 66 of 1995 • Occupational Health and Safety Act 85 of 1993 • Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000 • Skills Development Act 97 of 1998 • Skills Development Levies Act 9 of 1999

Company reporting and Company related records as far as is allowed in terms of these Acts	• Companies Act 71 of 2008 • Short-term Insurance Act 53 of 1998 • Financial Advisory and Intermediary Services Act 37 of 2002 • Insurance Act 18 of 2017

PGCO Advisory Incorporated Information Officer will take into consideration section 9 of the manual to decide on whether or not access to any of the information stated above should be given to the requester.

6. CATEGORIES OF RECORDS OF INFORMATION WHICH ARE AVAILABLE WITHOUT A PERSON HAVING TO REQUEST ACCESS

Before submitting a request in terms of PAIA, a data subject who is a customer of PGCO Advisory Incorporated should consider whether other mechanisms for receiving their information are available. All PGCO Advisory Incorporated customers are allowed to access their own policy related information without lodging a formal PAIA request.

CATEGORY OF RECORDS	TYPE OF RECORDS	AVAILABLE ON REQUEST
1. Records policyholders are entitled to:	1. Policy information relating to client's policy, such as policy schedule, policy wording, premium payment and claims history	Yes
2. Information business partners are entitled to:	2. Information relating to business partner's contracts, application forms and payments.	Yes
3. Information employees are entitled to:	3.Employment Contract Information	Yes
4. Company related records	4.Annual financial statements	Yes

7. DECISION-MAKING PROCESS

7.1 The PGCO Advisory Incorporated Information Officer will request PGCO Advisory Incorporated to take all reasonable steps to find a record that has been requested. If the record cannot be found or does not exist, PGCO Advisory Incorporated will cause notification to the requester be submitted by way of affidavit or affirmation, that it is not possible to give access to the record. This is deemed to be a refusal of the request. If,

however, the record is found later, the requester must be given access if the request would otherwise have been granted.

The Information Officer will within 30 days of receipt of a correctly completed request, notify the requester of the decision as to whether to grant the request.

If the request is:

Granted: the notification must state the applicable access fee (if any) required to be paid upon access, and that the requester has the right to lodge a complaint with the Information Regulator or lodge an application to court against the fee and provide the procedure to be followed should the requester wish to apply to court or lodge a complaint with the Information Regulator against the decision. The form of access must also be disclosed in the notice. The notice should also state that the requester will be given access to the record after the expiry of the 30-day period unless a complaint to the Information Regulator or an application with a court is lodged within that period.

Declined: the notification must include adequate reasons for the decision, together with the relevant provisions of the Act relied upon, and that the requester has the right to lodge a complaint with the Information Regulator or lodge an application to court against the refusal and provide the procedure to be followed should the requester wish to apply to court or lodge a complaint with the Information Regulator against the decision.

7.2 PGCO Advisory Incorporated Information Officer may extend the period of 30 days by a further period not exceeding 30 days if:

7.2.1. the request is for a large number of records or requires a search through a large number of records;

7.2.2. the request requires a search for records located in a different office of PGCO Advisory Incorporated not situated in the same city;

7.2.3. consultation between divisions of PGCO Advisory Incorporated, or with another private body is required; or

7.2.4. the requester consents to the extension.

The requester must be notified within the initial 30-day period in writing of the extension, together with reasons therefor, and that the requester may lodge a complaint with the Information Regulator or lodge an application to Court against the extension and the procedure to be followed.

The PGCO Advisory Incorporated Information Officer's failure to respond to the requester within the 30-day period constitutes a deemed refusal of the request.

7.3 The PGCO Advisory Incorporated Information Officer may sever a record and grant access only to that portion which the law does not prohibit access to.

If access is granted, access must be given in the form that is reasonably required by the requester, or if the requester has not identified a preference, in a form reasonably determined by The PGCO Advisory Incorporated Information Officer.

8. THIRD PARTIES

If the request is for a record pertaining to a third party, The PGCO Advisory Incorporated Information Officer must cause all reasonable steps to be taken to inform that third party of the request. This must be done within 21 days of receipt of the request. The way this is done must be in the fastest means reasonably possible, but if orally, it must thereafter give the third party a written confirmation of the notification. The third party may within 21 days thereafter either make representation to PGCO Advisory Incorporated as to why the request should be refused, alternatively grant written consent to the disclosure of the record. The third party must be advised of the decision taken.

On whether to grant or decline the request and must also be advised of his/her/its right to appeal against the decision by way of application to court within 30 days after the notice.

9. GROUNDS FOR REFUSAL OF A REQUEST

Notwithstanding compliance with section 50, the request may be declined in accordance with one of the prescribed grounds in terms of the Act, namely:

9.1 The Act prohibits the unreasonable disclosure of the personal information of natural-person third parties to requesters. This includes the personal information of deceased persons. However, Section 63(2) of the Act does provide exceptions to this.

9.2 A request must be refused if it relates to records containing third party information pertaining to:

9.2.1. trade secrets;

9.2.2. financial, commercial, scientific or technical information where disclosure would be likely to cause harm to the commercial or financial interests of that third party; or

9.2.3. information, supplied in confidence by the third party, the disclosure of which could reasonably be expected to put the third party at a disadvantage in contractual or other negotiations, or prejudice the third party in commercial competition.

The information must, however, be released if it pertains to the results of product or environmental testing, the disclosure of which would reveal a serious public safety or environmental risk.

9.3 The Act prohibits disclosure of information if such disclosure would constitute a breach of any duty of

confidentiality owed to a third party in terms of an agreement.

9.4 A request for access to a record held by PGCO Advisory Incorporated must be refused if disclosure could reasonably be expected to:

9.4.1. endanger the life or physical safety of an individual;

9.4.2. prejudice or impair the security of a building, structure or system, including but not limited to a computer or communication system, means of transport or any other property.

The PGCO Advisory Incorporated may also refuse a request for access to information that would prejudice methods, systems, plans or procedures for the protection of an individual in accordance with a witness protection scheme or safety of the public.

9.5 A refusal of a request is mandatory if the record is privileged from production in legal proceedings, unless the person entitled to the privilege has waived the privilege.

9.6 Access to records containing information about PGCO Advisory Incorporated itself is not mandatory, but rather discretionary. The PGCO Advisory Incorporated may refuse access to a record if the record:

9.6.1. contains trade secrets of PGCO Advisory Incorporated;

9.6.2. contains financial, commercial, scientific or technical information, the disclosure of which would be likely to cause harm to the commercial or financial interests of PGCO Advisory Incorporated;

9.6.3. contains information which, if disclosed, could reasonably be expected to put PGCO Advisory Incorporated at a disadvantage in contractual or other negotiations, or prejudice PGCO Advisory Incorporated in commercial competition; or consists of a computer program owned by PGCO Advisory Incorporated;

Notwithstanding the above, the information must be released if it pertains to the results of product or environmental testing, the disclosure of which would reveal a serious public safety or environmental risk.

9.7 The disclosure of information about research where disclosure is likely to expose the third party, the person conducting the research on behalf of the third party, or the subject matter of the research to serious disadvantage is prohibited. Disclosure is discretionary if such research pertains to PGCO Advisory Incorporated itself.

Notwithstanding any of the above-mentioned provisions, a record must be disclosed if its disclosure would:

9.7.1. reveal evidence of a substantial contravention of or failure to comply with the law, imminent and serious public safety or environmental risk; and

9.7.2. if the public interest in the disclosure clearly outweighs the harm.

10. RIGHTS OF APPEAL

A requester that is dissatisfied with the refusal to grant access to any information may, within 30 days of notification of the decision, apply to court for relief. Likewise, a third party dissatisfied with the decision to grant a request may, within 30 days of notification of the decision, apply to court for relief.

It should be noted that notwithstanding any provision in this Act, the court may examine the record(s) in question. No record may be withheld from the court on any grounds. The court may not, however, disclose the contents of the record(s).

The court is empowered to grant any order that is just and equitable, including:

10.1. confirming, amending or setting aside the decision;

10.2. requiring the information officer to take any action, or refrain from taking any action as identified by the court within a specified period;

10.3. granting an interdict, interim or special relief, declaratory order or compensation; or

10.4. an order as to costs.

11. PROCESSING OF PERSONAL INFORMATION IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT NO 4 OF 2013

11.1 PGCO Advisory Incorporated must collect and use information, including personal information as defined in the Protection of Personal Information Act, to the extent that it is necessary to properly perform the functions, obligations and duties and its obligations towards data subjects and as a financial firm.

11.2 PGCO Advisory Incorporated processes personal information of the following data subject categories:

11.2.1 Employees and job applicants

11.2.2 Third party suppliers

11.2.3 Regulatory bodies

11.2.4 Business partners with whom PGCO Advisory Incorporated has a business arrangement

11.2.5 Policyholders

11.3 The purpose of the processing personal information PGCO Advisory Incorporated collects and processes personal information:

11.3.1. to meet our responsibilities to our customers;

11.3.2. to meet our responsibilities to employees;

11.3.3. to meet our contractual responsibilities to third party service providers;

11.3.4. to inform customers of products and services;

11.3.5. to comply with all legal and regulatory requirements, including industry codes of conduct;

11.3.6. to protect and pursue the legitimate interests of PGCO Advisory Incorporated in the conducting of its business within the Group or third parties to whom personal information is provided; and

11.3.7. for any further purposes related to the above.

11.4 The recipients or categories of recipients to whom the personal information may be supplied.

CATEGORY OF PERSONAL INFORMATION	**RECIPIENTS OR CATEGORIES OF RECIPIENTS TO WHOM THE PERSONAL INFORMATION MAY BE SUPPLIED**
Policyholder policy information; Company documents; Annual financial statements; statutorily required reports	Regulatory authorities
Contracts with third party partners	Any legal or juristic person with an appropriate legal basis
Product performance; policy documentation	Brokers, advisers, or intermediaries
Investigation	Law enforcement agencies
Contracts with third party partners	Third party service providers
Financial, payroll, and transactional records	Authorised sub-processors and Operators (including Xero, Dext, SimplePay, and Anthropic, PBC)

11.5 The following categories of personal information are processed to fulfil the functions.

1. First Name 2. Middle Name 3. Last Name 4. Initials 5. If disclosure of the name itself would reveal information about the person 6. Email-Address 7. Physical address 8. Telephone Number	GENERAL CONTACT AND INFORMATION

9. Location information 10. Online Identifier	
11. Any Identifying number 12. Identifying symbol 13. Other particular assignment to a person 14. The name of the person if it appears with other personal information relating to the person 15. Birth of the person 16. Age	ID/PASSPORT NUMBER/ POLICY NUMBER AND DATE OF BIRTH
17. Personal opinions 18. Personal views 19. Personal preferences 20. Views/opinions of/another individual about a person 21. Beliefs/philosophical beliefs 22. Conscience 23. Political persuasion	**VIEWS, ASSESSMENTS, OPINIONS, RECOMMENDATIONS**
24. Marital status	**MARITAL STATUS**
25. Financial History	**FINANCIAL HISTORY**
26. Employment History	**EMPLOYMENT HISTORY**
27. Correspondence sent of a private or confidential Nature	**CORRESPONDENCE SENT OF A PRIVATE OR CONFIDENTIAL NATURE**
28. Medical history 29. Physical History 30. Mental Health 31. Well-being 32. Disability 33. Blood Type 34. Pregnancy	MEDICAL INFORMATION
35. Race / Colour 36. Gender 37. Nationality 38. Ethnic Origin 39. Social Origin	**GENDER / ETHNICITY/NATIONALITY**

40. Criminal History	**CRIMINAL HISTORY**
41. Culture 42. Language 43. Education 44. Religion	LANGUAGE/EDUCATION/ CULUTRE/ RELIGION
45. Sex life	SEX ORIENTATION/LIFE
46. Sexual Orientation	SEX ORIENTATION
47. Trade Union Membership	TRADE UNION MEMBERSHIP
48. Biometric information	BIOMETRICE INFORMATION

11.6 Planned transborder flows of personal information

Further processing and storage may require the PGCO Advisory Incorporated send personal information to service providers outside of the Republic of South Africa. PGCO Advisory Incorporated will not send your information to a country that does not have information protection legislation similar to that of the RSA, unless we have ensured that the recipient agrees to effectively adhere to the principles for processing of information in accordance with the Protection of Personal Information Act No 4 of 2013.Where appropriate, we request the third parties with whom we share information, to take adequate measures and comply with applicable data protection laws and protect the information we are disclosing to them. We do this through contractual arrangements with these third parties. We also take internal measures to ensure that the third parties we appoint have appropriate measures to protect the information we provide to them.

11.7 The PGCO Advisory Incorporated employs security controls, electronic and physical that are designed to maintain confidentiality, prevent loss of unauthorised access and damage to information by unauthorised parties. The cyber security strategy of PGCO Advisory Incorporated is aligned to industry standard frameworks to ensure effective cyber security risk management for the organisation.

11.8 Data subjects have the following remedies where there's interference with the protection of their personal information by PGCO Advisory Incorporated:

11.8.1 Lodge a complaint with PGCO Advisory Incorporated Client Care Department yulesen@pgco.co.za.

11.8.2 Institute civil action for damages in a court having jurisdiction.

11.9 PGCO Advisory Incorporated Information Privacy Policy is available on PGCO Advisory Incorporated website.

12. PGCO ADVISORY INCORPORATED INFORMATION SECURITY MEASURES

PGCO Advisory Incorporated employs security controls, electronic and physical that are designed to maintain confidentiality, integrity and availability of information as well as prevent loss or unauthorised access and damage to information by unauthorised parties. PGCO Advisory Incorporated cyber security strategy is aligned to industry standard frameworks to ensure effective cyber security risk management for the organisation. Information security is achieved by implementing a suitable set of responsibilities, controls, standards, processes and systems to ensure that the information security objectives and measures of PGCO Advisory Incorporated are met.

Signed at Sandton on this 9th day of June 2026.

_____

Information Officer

FORM 2 | REQUEST FOR ACCESS TO RECORD

[Regulation 7]

NOTE:

1. Proof of identity must be attached by the requester.

2. If requests made on behalf of another person, proof of such authorisation, must be attached to this form.

TO: The Information Officer

Address: _____

E-mail address: _____

Fax number: _____

Mark with an "X"

Request is made in my own name

Request is made on behalf of another person.

PERSONAL INFORMATION	
Full Names	
Identify Number	
Capacity in which request is made (when made on behalf of another person)	
Postal address	
Street address	
Email address	
Contact numbers	Tel:
	Cell:
Full name of person on whose behalf request is made (if applicable)	
Identity Number:	
Postal address	
Street address	
Email address	
Contact numbers	Tel:
	Cell:
PARTICULARS OF RECORD REQUESTED Provide full particulars of the record to which access is requested, including the reference	

number if that is known to you, to enable the record to be located. *(If the provided space is inadequate, please continue on a separate page and attach it to this form. All additional pages must be signed.)*	
Description of record or relevant part of the record:	
Reference number, if available	
Any further particulars of record:	
TYPE OF RECORD MARK THE APPLICABLE BOX WITH AN X	
Record is in written or printed form	
Record comprises virtual images *(this includes photographs, slides, video recordings, computer generated images, sketches, etc.)*	
Record consists of recorded words or information which can be reproduced in sound	
Record is held on a computer or in an electronic, or machine-readable form	
Printed copy of record *(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)*	
Written or printed transcription of virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc.)*	
Transcription of soundtrack *(written or printed document)*	
Copy of record on flash drive *(including virtual images and soundtracks)*	
Copy of record on compact disc drive *(including virtual images and soundtracks)*	
Copy of record saved on cloud storage server	
MANNER OF ACCESS (Mark the applicable box with an X)	
Personal inspection of record at registered address of public/private body *(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form*	
Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format (including transcriptions)	
E-mail of information (including soundtracks if possible)	
Cloud share/file transfer	
Preferred language *(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)*	

PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED If the provided space is inadequate, please continue on a separate page and attach it to this form. The requester must sign all the additional pages.	
Indicate which right is to be exercised or protected:	
Explain why the record requested is required for the exercise or protection of the aforementioned right:	
FEES	
a) A request fee must be paid before the request will be considered. b) You will be notified of the amount of the access fee to be paid. c) The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record. d) If you qualify for exemption of the payment of any fee, please state the reason for exemption.	

REASON:

_____

_____

_____

You will be notified in writing whether your request has been approved or denied and if approved the costs relating to your request, if any. Please indicate your preferred manner of correspondence:

Postal Address	Fax	Email

Signed at_____ on this _____ day of _____ 20

_____

Signature of Requester/person on whose behalf request is made

PGCO
Accounting I Tax I Advisory
www.pgco.co.za

FOR OFFICE USE ONLY

Reference Number:	
Request received by:	
Date Received:	
Access Fees:	
Deposit (if any)	

_____

Signature of Information Officer

FORM 3 | OUTCOME OF REQUEST AND OF FEES PAYABLE

[Regulation 8]

NOTE:

1. If your request is granted the

(a) amount of the deposit, (if any), is payable before your request is processed; and

(b) requested record/portion of the record will only be released once proof of full payment is received.

2. Please use the reference number hereunder in all future correspondence.

Reference number:

_____

TO:

_____

Your request dated refers.

_____

1. You requested:

Personal inspection of information at registered address of public/private body (including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form) is free of charge. You are required to make an appointment for the inspection of the information and to bring this Form with you. If you then require any form of reproduction of the information, you will be liable for the fees prescribed in Annexure B.	

2. You requested:

Printed copies of the information *(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)*	
Written or printed transcription of virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc.)*	
Transcription of soundtrack *(written or printed document)*	
Copy of information on flash drive *(including virtual images and soundtracks)*	
Copy of information on compact disc drive *(including virtual images and soundtracks)*	

Copy of record saved on cloud storage server	

3. To be submitted:

Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format *(including transcriptions)*	
E-mail of information *(including soundtracks if possible)*	
Cloud share/file transfer	
Preferred language: *(Note that if the record is not available in the language you prefer, access may be*	

Kindly note that your request has been:

1. Approved; or

2. Denied, for the following reasons:

_____

_____

4. Fees payable with regards to your request:

Item	Cost Per A4 size page	Number of pages / items	Total
Photocopy			
Printed Copy			
For a copy in a computer-readable form on: (i) Flash drive To be provided by requestor (ii) Compact disc If provided by requestor If provided to the requestor			
For a transcription of visual images per A4-size page	Service to be outsourced.		
Copy of visual images	Copy of visual images Will depend on		

	the quotation of the service provider.		
Transcription of an audio record, per A4-size			
Copy of an audio record (i) Flash drive To be provided by requestor (ii) Compact disc If provided by requestor If provided to the requestor			
Postage, e-mail or any other electronic transfer:	Actual costs		

5. Deposit Payable (if search exceeds 6 hours)

Yes No

Hours of search		Amount of deposit *(Calculated on one third of total amount per request)*	

The amount must be paid into the following Bank account:

Name of bank:

_____

Name of account holder:

_____

Type of account:

_____

Account number:

_____

Branch code:

_____

Reference number:

_____

Submit proof of payment to:

_____

Signed at _____ this _____ day of _____ 20 ___.

_____

Signature of Information Officer